İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

802.11 TELSİZ YEREL BİLGİSAYAR AĞLARINDA GÜVENLİK

YÜKSEK LİSANS TEZİ

Müh. Zafer BAYRAKTAR
(504011419)

Tezin Enstitüye Verildiği Tarih : 9 Mayıs 2005
Tezin Savunulduğu Tarih : 2 Haziran 2005

Tez Danışmanı : **Prof.Dr. Bülent ÖRENCİK (İ.T.Ü)**
Diğer Jüri Üyeleri: **Yrd.Doç.Dr. Osman Kaan EROL (İ.T.Ü)**
Yrd.Doc.Dr. Gökhan Yavuz (Y.T.Ü)

MAYIS 2005

ÖNSÖZ

Tez çalışmalarım süresince göstermiş olduğu anlayış ve yardımlardan dolayı tez danışmanım sayın Prof. Dr. Bülent ÖRENCİK' e, anlayışlarından dolayı TÜBİTAK-UEKAE bünyesindeki idarecilerime, yardımlarından dolayı çalışma arkadaşlarıma, tez kitapçığının hazırlanması ve güncellenmesindeki yardımlarından dolayı kardeşim Zikri Bayraktar' a teşekkürlerimi sunarım.

Hayatımın her anında olduğu gibi tez çalışmalarım boyunca da benden yardımlarını esirgemeyen eşim ve aileme sevgi ve saygılarımı sunarım.

Mayıs 2005 Zafer BAYRAKTAR

İÇİNDEKİLER

Sayfa No

KISALTMALAR

AAD	: Additional Authentication Data, Ek Bütünlük-Kimlik Doğrulama Değeri
ABD	: Amerika Birleşik Devletleri
ACK	: Acknowledgement, Alındı bildirisi
AES	: Advanced Encryption Standart, Gelişmiş Şifreleme Standardı
ANSI	: American National Standarts Institute, Amerikan Ulusal Standartlar Enstitüsü
AP	: Access Point, Erişim Noktası
BSS	: Basic Service Set, Temel Hizmet Tanımlayıcı
CBC	: Cipher Block Chaining, Blok Zincirleme
CBC-MAC	: Cipher Block Chaining – Message Authentication Code, Blok Zincirleme Mesaj Bütünlüğü Algoritması
CCM	: Counter with CBC-MAC, Sayaçlı CBC-MAC
CCMP	: Counter with CBC-MAC Protocol, Sayaçlı CBC-MAC protokolü
CDMA	: Code Division Multiple Access, Kod Bölmelemeli Çoklu Erişim
CRC	: Cyclic Redundancy Check, Çevrimli Fazlalık Sınaması
CSMA	: Carrier Sense Multiple Access, Taşıyıcı Hissetmeli Çoklu Erişim
CSMA / CD	: Carrier Sense Multiple Access with Collision Detection, Çatışma Sezmeli Taşıyıcı Hissetmeli Çoklu Erişim
CSMA / CA	: Carrier Sense Multiple Access with Collision Avoidance, Çatışma Engellemeli Taşıyıcı Hissetmeli Çoklu Erişim
CTS	: Clear To Send, Gönderim Uygun
DoS	: Denail of Service, Hizmet Aksatmaya Yönelik Saldırılar
DSSS	: Direct Sequence Spread Spectrum, Düz Sıralı Dağınık Spektrum
EAP	: Extensible Authentication Protocol, Genişletilebilir Asıllama Protokolü
EAPOL	: EAP over LAN, Yerel Alan Ağları üzerinde EAP
ESS	: Extended Service Set, Genişletilmiş Hizmet Tanımlayıcı
ETSI	: European Telecommunications Standards Institute, Avrupa Telekomünikasyon Standartları Enstitüsü
FHSS	: Frequency Hopping Spread Spectrum, Frekans Atlamalı Dağınık Spektrum
GHz	: Giga Hertz (10^9 Hertz)
GMK	: Group Master Key, Grup Ana Anahtarı
GNU	: GNU Not Unix, Unix benzeri özgür yazılım işletim sistemi (GNU Unix değildir)
GSM	: Global System for Mobile
GTK	: Group Transient Key, Grup Geçici Anahtarı
GUI	: Graphical User Interface, Grafiksel Kullanıcı Arayüzü
HiperLAN	: High Performance Radio LAN, Yüksek Performanslı Radyo Yerel Alan Ağı
HMAC	: Keyed-Hashing for Message Authentication Code, Anahtarlı Mesaj

	Bütünlüğü Sınaması Özet Değeri
IANA	: Internet Assigned Numbers Authority, Internet atanmış sayılar kurumu
IBSS	: Independent Basic Service Set, Bağımsız Temel Servis Tanımlayıcı
ICMP	: Internet Control Message Protocol, Internet Kontrol Mesajları Protokolu
ICV	: Integrity Check Value, Bütünlük Sınaması Kontrolü Değeri
IE	: Informatin Element, Bilgi Elemanı (BE)
IEEE	: Institute of Electrical and Electronics Engineers, Elektrik ve Elektronik Mühendisleri Enstitüsü
IETF	: Internet Engineering Task Force, Internet Mühendisliği Çalışma Grubu
IDE	: Integrated Development Environment, Tümleşik Geliştirme Ortamı
IP	: Internet Protocol, Internet Protokolü
IPsec	: Security Architecture for the Internet Protocol, IP Güvenlik Mimarisi
ISM	: Industrial, Scientific and Medicine Band, Endüstriyel, Bilimsel ve Sağlık bandı
IV	: Initialization Vector, İlklendirme Vektörü
Kbps	: Kilobits per second, Saniyede aktarılan kilobit sayısı
KCK	: Key Confirmation Key, Anahtar Bütünlük Anahtarı
KEK	: Key Encryption Key, Anahtar Şifreleme Anahtarı
LAN	: Local Area Network, Yerel Alan Ağı (YAA)
LLC	: Logic Link Control, Mantıksal Bağlantı Kontrolü
MAC	: Medium Access Control, Ortam Erişim Kontrolü
Mbps	: Megabits per second, Saniyede aktarılan megabit (10^6 bit) sayısı
MD5	: Message Digest 5, Mesaj Özeti Algoritması 5
MIC	: Message Integrity Code, Mesaj Bütünlük Sınaması Değeri
NIST	: National Institute of Standarts and Technology, ABD Standartları ve Teknoloji Enstitüsü
OFDM	: Orthogonal Frequency Division Multiplexing, Dikey Frekans Bölmeli Çoklama
OSI	: Open Sistem Interconnection, Açık Sistem Arabağlaşım
PMK	: Pairwise Master Key, Karşılıklı haberleşme Ana Anahtarı
PRNG	: Pseudo Random Number Generator, Sözde Rasgele Sayı Üreteci
PPP	: Point to Point Protocol, Uçtan-Uca haberleşme Protokolü
PSK	: Pre Shared Key, Ön Paylaşımlı Anahtar
PTK	: Pairwise Transient Key, Karşılıklı haberleşme Geçici Anahtarı
QoS	: Quality of Service, Servis Kalitesi
RADIUS	: Remote Authentication Dial-In User Service, Çevirmeli Ağ Kullanıcı Asıllama Protokolü
RC4	: Rivest Cipher 4, Rivest Şifreleme Algoritması – 4
RFC	: Request For Comment
PRF	: Pseudo Random Function, Sözde Rasgele Fonksiyonu
RSA	: Rivest-Shamir-Adleman Güvenlik Firması
RSN	: Robust Security Network, Sağlam Güvenlikli Ağ
RTS	: Request To Send, Gönderim İsteği
SHA1	: Secure Hash Algoritm, Güvenli Özet Algoritması
TCP/IP	: Transmission Control Protocol / Internet Protocol
TK	: Temporal Key, Geçici Anahtar

TLS	: Transport Layer Security, Ulaşım Katmanı Güvenlik Protokolü
TKIP	: Temporal Key Integrity Protocol, Geçici Anahtar Bütünlüğü Protokolü
TTAK	: TKIP mixed Transmit Address and Key
UDP	: User Datagram Protocol
WEP	: Wired Equivalent Privacy, Kablolu Eşdeğer Güvenlik Protokolü
WLAN	: Wireless LAN, Telsiz YAA
WMAN	: Wireless Metropolitan Area Network, Telsiz Kampus Ağları
WPAN	: Wireless Personal Area Network, Telsiz Kişisel Alan Ağı
WPA	: Wireless Protected Access, Telsiz Korumalı Erişim Protokolü
WWAN	: Wireless Wide Area Network, Telsiz Geniş Alan Ağı
XOR	: Exclusive OR, Dışlamalı veya işlemi

TABLOLAR

Sayfa No

ŞEKİLLER

Sayfa No

802.11 TELSİZ YEREL BİLGİSAYAR AĞLARINDA GÜVENLİK

ÖZET

Telsiz bilgisayar ağları sağladığı kolay kurulum, kolay genişletilebilirlik, gezginlik gibi avantajlarıyla kullanıcıların ilgisini çekmektedir. Gelişen teknoloji, artan aktarım hızları ve üreticiler arası gidilen standardizasyon çalışmalarıyla gün geçtikçe daha fazla uygulama alanı bulmakta ve kullanıcılara sağladığı avantajlar ve telsiz ağ ürünlerinin fiyatlarındaki düşüşe bağlı olarak da kullanıcı sayıları hızla artmaktadır.

Telsiz yerel bilgisayar ağlarında kullanılan farklı standartlar tanımlı olsa da günümüzde yaygın olarak kullanılan ve telsiz bilgisayar ağlarının günümüzde yakalamış olduğu popülerliği sağlamış olan telsiz yerel bilgisayar ağı standardı IEEE tarafından tanımlanmış olan IEEE 802.11 standardıdır.

Kullanıcılarına sunduğu hizmetlerin yanı sıra aktarım ortamı olarak kullanılan hava ortamının herkes tarafından erişilebilir ve izlenebilir olması telsiz bilgisayar ağlarının kullanıcı veri gizliliğini sağlamasını da şart koşar. Bu amaçla IEEE 802.11-1999 standardında karşılıklı kimlik doğrulama ve veri kapsülleme yöntemleri tanımlanmıştır. Ancak 2000' li yılların başlarında yapılan araştırmalar 802.11-1999 standardında tanımlı güvenlik mekanizmalarının sağladığını iddia ettikleri veri gizliliğini sağlamaktan uzak olduğunu ortaya koymuştur. Mevcut güvenlik sorunlarının ortadan kaldırılması amacıyla IEEE tarafından 802.11i adı altında bir çalışma grubu oluşturulmuştur. Yaklaşık dört yıllık bir çalışmanın sonunda 2004 yılında IEEE 802.11i-2004 güvenlik standardı duyurulmuştur.

Tez çalışmaları kapsamında gerek IEEE 802.11-1999 standardında tanımlı güvenlik mekanizmalarının neler olduğu ve sorunları incelenmiş gerekse yeni duyurulan telsiz bilgisayar ağları güvenlik standardı IEEE 802.11i' in getirdiği mekanizmalar ve güvenlik önlemleri incelenmiştir.

Ayrıca 802.11 ağları için bir benzetim programı yazılmıştır. Hazırlanan benzetim yazılımı ile 802.11 ağları bilgisayar ortamında gerçeklenmiş ve bir kullanıcının haberleşmeye geçiş aşamaları gösterilmiştir. Yeni önerilen veri kapsülleme mekanizmalarının da gerçeklendiği benzetim yazılımı böylelikle 802.11i standardının getirmiş olduğu tüm yenilikleri kapsar.

Hazırlanan benzetim yazılımı ile 2004 yılında duyurulmuş olan 802.11i güvenlik mimarisi incelenmiş ve getirdiği mekanizmalar teker teker ele alınmıştır. Böylelikle çok yeni bir standart olan IEEE 802.11i-2004 standardının tüm adımları ayrıntılı olarak analiz edilmeye ve olası eksikleri bulunmaya çalışılmıştır.

802.11 WIRELESS LOCAL AREA NETWORK SECURITY

SUMMARY

Nowadays, wireless computer networks catch the attention of many customers with their advantages. They are mobile, easy to install and easy to expand. Wireless computer networks technology finds many new applications as data transfer capabilities improve and cooperation among the hardware/software producers, via standardization, increases. Also, depending on the hardware price drops, the number of users increases rapidly.

Wireless local area computer networks can run on various standards, but only one of them is used widely which is the main reason of these networks' popularity today. This wireless local area network standard is IEEE 802.11 standard.

In addition to their various advantages, wireless computer networks are expected to provide with data security. The medium for data transfer in these networks is the air, which gives access to any data to anyone. This eases data sniffing. To provide security, IEEE 802.11-1999 standard requires two ways authentication and data encapsulation. However, in year 2000, some published studies pointed out that IEEE 802.11-1999 standard is far away from providing any security as it have claimed. To fix the security holes and related security problems, IEEE established 802.11i research group and after four years of research, in 2004, this group announced IEEE 801.11i-2004 standard.

This thesis studies the security protocol in IEEE 802.11-1999 standard and investigates the related problems along with the new security protocol and its measure in the new 802.11i standard.

Also, a simulation program is written for the 802.11 networks. In this program, 802.11 wireless networks are simulated on a computer environment and the stages of a user communication over the network are shown. This simulation program mimics and runs all the new security measures announced in 802.11i standard including the new data encapsulation mechanism.

The security architecture and other mechanisms of new 802.11i standard are investigated individually in this thesis. Thus, this thesis sequentially analyses each step of the new standard and explores the security shortcomings.

1 GİRİŞ

Telsiz bilgisayar ağları sağladığı avantajlarla kullanıcıların ilgisini çekmekte, artan aktarım hızları ve üreticiler arası gidilen standardizasyon çalışmalarıyla gün geçtikçe daha fazla uygulama alanı bulmakta ve telsiz ağ ürünlerinin fiyatlarındaki düşüşe bağlı olarak da kullanıcı sayıları hızla artmaktadır.

Telsiz bilgisayar ağlarında kullanılabilecek farklı standartlar tanımlı olsa da günümüzde yaygın olarak kullanılan telsiz yerel bilgisayar ağı standardı IEEE tarafından tanımlanmış olan IEEE 802.11 standardıdır.

Kullanıcılarına sunduğu hizmetlerin yanı sıra aktarım ortamı olarak kullanılan hava ortamının herkes tarafından erişilebilir ve izlenebilir olması telsiz bilgisayar ağlarının kullanıcı veri gizliliğini sağlamasını da şart koşar. Bu amaçla IEEE 802.11-1999 [1] standardında karşılıklı kimlik doğrulama ve veri kapsülleme yöntemleri tanımlanmıştır. Ancak 2000' li yılların başlarında yapılan araştırmalar 802.11-1999 standardında tanımlı güvenlik mekanizmalarının zayıflıklarını ortaya koymuştur. Mevcut güvenlik sorunlarının ortadan kaldırılması amacıyla IEEE tarafından 802.11i adı altında bir çalışma grubu oluşturulmuştur. Yaklaşık dört yıllık bir çalışmanın sonunda 2004 yılında IEEE 802.11i-2004 [2, 3, 4] güvenlik standardı duyurulmuştur.

Bu çalışma IEEE 802.11 telsiz yerel bilgisayar ağlarında güvenliğin sağlanmasına yönelik yapılmış çalışmaları ve eksiklerini incelemek üzere yapılmıştır. Bu amaçla öncelikle eski güvenlik mekanizmaları ve zayıflıkları incelenmiş daha sonra yeni getirilen IEEE 802.11i standardı ele alınmıştır. Hazırlanan benzetim yazılımı ile yeni güvenlik standardı gerçeklenmiş ve bilinen aktif saldırılar yeni protokol üzerinde denenmiştir.

Tez kitapçığında öncelikle telsiz bilgisayar ağları hakkında kısaca bilgi verilecek üçüncü bölümde IEEE 802.11-1999 standardındaki güvenlik mekanizmaları ve problemleri ele alınacaktır. Dördüncü bölümde 802.11i-2004 standardı ile güvenlik mekanizmalarında getirilen yenilikler ele alınacak ve tanımlanan yeni paket kapsülleme mekanizmaları beşinci ve altıncı bölümlerde incelenecektir. Yedinci

bölüm hazırlanan benzetim yazılımı hakkında kısaca bilgilendirme içerir. Son bölüm elde edilen sonuçlara ve ileriki çalışmalar için önerilere ayrılmıştır. Ek-A' da hazırlanan benzetim yazılımına ait tüm kaynak kodlar bulunabilir.

2 TELSİZ BİLGİSAYAR AĞLARI

Telsiz bilgisayar ağları birden fazla sayıda cihazın kablo olmaksızın veri haberleşmesinde bulunmasını sağlayan yapıyı ifade eder. Telsiz bilgisayar ağları 1990'lı yılların başlarından itibaren kullanılmaya başlanmış ancak gerek düşük aktarım hızları gerekse birlikte çalışabilirlik problemleri nedeniyle gerekli ilgiyi görmemiştir. 1990'lı yılların ikinci yarısından itibaren gerçekleştirilen çalışmalarda firmalar arası standardizasyona gidilmesiyle ve yüksek hızlarda veri aktarımını sağlayabilir hale gelmesiyle gittikçe genişleyen uygulama alanı bulmuşlardır.

Telsiz bilgisayar ağlarının kullanıcılara sunduğu avantajlar aşağıdaki gibi sıralanabilir:[5]

- Telsiz bilgisayar ağları kullanıcılara nerde olurlarsa olsunlar, hareket etseler dahi veri iletişimini sürdürebilmeleri imkanını sunar.
- Kablolama işlemlerinin zor veya pahalı olduğu tarihi binalar, hava alanları gibi ortamlarda kolay kurulabilir olması ve kablolamanın oluşturacağı görüntü kirliliğini yaratmayacak olması telsiz bilgisayar ağlarının tercih edilmesini sağlar. Ayrıca geçici amaçla kurulacak haberleşme ağını kolayca gerçekleştirebiliyor olması bir avantaj teşkil eder.
- Değişken sayıda kullanıcının olacağı ortamlarda ortama yeni katılacak bir kullanıcı için fazladan bir işlem gerektirmemesi ve yeni kullanıcının doğrudan telsiz ağa erişebilir olması telsiz bilgisayar ağlarının bir başka üstün özelliğidir.
- Kablolama maliyeti gerektirmemesi, olası kablo kopması ve bağlantı ek noktalarındaki arıza olasılığı gibi olasılıkları taşımaması nedeniyle işletim ve bakım maliyetleri düşüktür. Ayrıca telsiz bilgisayar ağı kurulumu için gerekli ekipmanların fiyatları da gün geçtikçe ucuzlamaktadır.

Telsiz bilgisayar ağları sağladıkları hizmetler, veri iletim hızları, ortam erişim mekanizmaları, büyüklükleri gibi özellikleri göz önünde bulundurularak farklı

kategorilere ayrılabilir. Kullanıcı açısından bakıldığında telsiz ağların kapsadıkları alan yani büyüklüklerine göre yapılacak bir sınıflandırma daha geçerli olacaktır. Büyüklüklerine göre telsiz ağlar Tablo 2-1'de 4 ana sınıf altında toplanmıştır:

Tablo 2-1: Büyüklüklerine göre telsiz ağların sınıflandırılması

1	Telsiz Geniş Alan Ağları (WWAN[1])	Ülke, kıta çapında
2	Telsiz Kampus Ağları (WMAN[2])	Bölge, kampus çapında
3	Telsiz Yerel Alan Ağları (WLAN[3])	Daire, bina çapında
4	Telsiz Kişisel Alan Ağları (WPAN[4])	Oda içerisi, küçük alanlar

Bu 4 ana sınıf için de tanımlanmış ve kullanılan birden fazla protokol mevcuttur. Tablo 2-2'de her bir sınıf için yaygın olarak kullanılan protokoller verilmiştir:[5]

Tablo 2-2: Telsiz ağ teknolojileri ve kullanılan standartlar

	WPAN	WLAN	WMAN	WWAN
Mesafe	Kısa	Orta	Orta-Uzun	Uzun
Hız	< 1 Mbps	1-54 Mbps	11-100 Mbps	10-384 Kbps
Standartlar	Bluetooth / HomeRF	IEEE 802.11 / HiperLAN	IEEE 802.16 / HiperMAN	GSM / CDMA

Tez kapsamında 802.11 telsiz yerel alan ağları güvenliği inceleneceğinden yalnızca telsiz yerel alan ağları ele alınacak diğer sınıflara ait protokollere değinilmeyecektir.

2.1 HiperLAN

HiperLAN (High Performance Radio LAN, Yüksek performanslı radyo yerel alan ağı) Avrupa ülkeleri için tasarlanan yüksek hızda veri aktarımına olanak sağlayan

[1] WWAN: Wireless Wide Area Network, Telsiz Geniş Alan Ağı
[2] WMAN: Wireless Metropolitan Area Network, Telsiz Kampus Alan Ağı
[3] WLAN: Wireless Local Area Network, Telsiz Yerel Alan Ağı
[4] WPAN: Wireless Personal Area Network, Telsiz Kişisel Alan Ağı

yerel alan ağı standardıdır. HiperLAN standardı ETSI (European Telecommunications Standards Institute, Avrupa Telekomünikasyon Standartları Enstitüsü) tarafından oluşturulmuştur ve HiperLAN1 ve HiperLAN2 olmak üzere iki tiptir. Her iki tipte 5-GHz bandında OFDM (Orthogonal Frequency Division Multiplexing, Dikgen frekans bölüşümlü çoklama) kodlama modülasyon yöntemi ile çalışmaktadır. [5]

HiperLAN1 20 Mbps' lik bir iletim hızına ulaşırken HiperLAN2 yine aynı frekans bandında 54 Mbps' lik veri iletim hızına erişmektedir. Benzer özellikler taşıdığı 802.11 standartları kadar yaygın kullanılmamaktadır.

2.2 IEEE 802.11

Telsiz bilgisayar ağlarında yaygın olarak kullanılan standart IEEE (Institute of Electrical & Electronic Engineers, Elektrik ve Elektronik Mühendisleri Enstitüsü) tarafından 1997 senesinde ilk olarak duyurulan IEEE 802.11 standardıdır. IEEE 802.11-1997 standardı 2.4 GHz frekans bandında 2 Mbps aktarım hızı sağlayabiliyordu. Aktarım hızının düşüklüğü nedeniyle fazla ilgi çekmemiştir. Daha sonra 1999 senesinde yine aynı frekans bandında çalışan ve 11 Mbps' lik bir veri aktarım hızına ulaşabilen 802.11b ve aynı sene içerisinde 5 GHz frekans bandında çalışan ve 54 Mbps' lik aktarım hızına erişen 802.11a standartları duyuruldu. 2003 senesinde 2.4 GHz frekans bandında çalışan ve 54 Mbps' lik aktarım hızına erişen 802.11g standardı duyuruldu. 802.11 standartları temel özellikleriyle Tablo 2-3'de verilmiştir:

Tablo 2-3: 802.11 standartları ve özellikleri

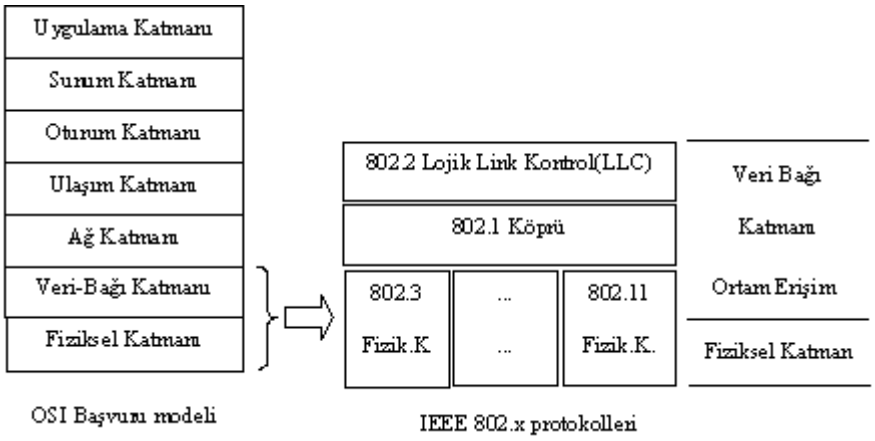
Standartlar	Frekans Bandı	Modülasyon	Veri Aktarım Hızı
802.11	2,4 GHz – ISM[1]	FHSS / DSSS	2 Mbps
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2,4 GHz – ISM	DSSS	11 Mbps
802.11g	2,4 GHz - ISM	DSSS / OFDM	54 Mbps

[1] ISM: Industrial, Scientific, Medical Band; Dünya çapında endüstriyel, bilimsel ve sağlık araştırmaları için ayrılmış band.

2.2.1 802.11 Standartlarının OSI Başvuru Modelindeki Yeri

OSI (Open System Interconnection, Açık Sistem Bağlaşım) başvuru modeli bilgisayar ağlarının birlikte çalışabilirliğinin sağlanması amacıyla haberleşme için yapılması gereken işlemlerin katmanlara bölünerek tanımlandığı bir başvuru modeli oluşturur. Her bir katman kendisine ait yapılması gereken işlemleri ve diğer katmanlarla olan bağlantı arayüzlerini tanımlar.

OSI başvuru modelindeki ilk iki katman dışındaki katmanların ağ mimarisinden ve kullanılan teknolojiden bağımsız olduğu ve gerek yerel alan ağlarında gerekse geniş alan ağlarında aynı olacak şekilde gerçekleştirilebileceği varsayılır. IEEE 802.x standartları yerel alan ağları için ilk iki katmanda yapılması gereken işlemleri ve kullanılacak teknolojileri tanımlar. Şekil 2-1, 802.x protokollerinin OSI başvuru modelindeki yerini gösterir:



Şekil 2-1: OSI Başvuru modelinde 802.11' in yeri

2.2.2 802.11 Ortam Erişim Denetimi Mekanizması

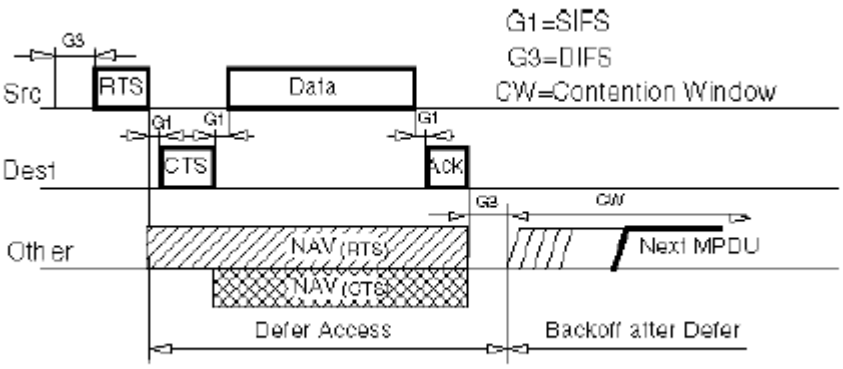
802.11 protokolleri MAC (Medium Access Control, Ortam erişim denetimi) protokolü olarak CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, Taşıyıcı dinleyen çoklu erişim/Çatışma Sakınım) kullanırlar.

CSMA mekanizması oldukça basittir, ortamı kullanarak veri göndermek isteyen bir düğüm öncelikle ortamın dolu olup olmadığını dinler. Eğer ortamda bir başka düğüme ait veri iletiliyorsa, yani ortam doluysa kendi gönderme işlemini bir süre erteleyerek tekrar göndermeye çalışır. Az sayıda düğüm veya haberleşme isteği az

olan çok sayıda düğümün bulunduğu ortamlarda çok etkili bir ortam denetim mekanizması sağlar.

CSMA erişim mekanizmasında çatışma olması her zaman mümkündür. Aynı anda ortamı dinleyen ve ortamın boş olduğunu fark ederek veri göndermek isteyen iki düğümün göndereceği veriler çatışacaktır. Böyle bir durumda düğümlerin çatışmayı fark ederek belirli bir algoritma uyarınca (üstel geri çekilme algoritması) bekleyerek tekrar gönderimi denemeleri gerekir. Çatışmanın sezilmesine CD (Collision Detection) adı verilir. Günümüzde yaygın olarak kullanılan Ethernet ve IEEE 802.3 yerel alan ağları protokolleri ortam erişimi mekanizması olarak CSMA/CD metodunu kullanırlar.

CSMA/CD mekanizması çeşitli nedenlerden dolayı telsiz ağlar için kullanışlı değildir. Örneğin aynı anda hem gönderim hem de alım yapacak antenlerin maliyeti çok fazla olacaktır. Bu nedenle telsiz bilgisayar ağlarında çatışma sezme yerine çatışma engelleme (CA-Collision Avoidance) mekanizması pozitif alındı bilgisi ile birlikte kullanılır ve bu mekanizmaya CSMA/CA adı verilir. CSMA/CA uyarınca ortama veri göndermek isteyen bir düğüm öncelikle ortamın boş olup olmadığını dinler. Ortam boş ise veri gönderiminde bulunacağı adrese veri gönderimi isteğini bildiren kısa bir kontrol paketi RTS (Request To Send, Gönderim isteği) gönderir. RTS içerisinde kaynak düğüm, hedef düğüm adresleri ve gönderim süresi yer alır. RTS alan hedef düğüm, bu mesaja CTS (Clear To Send, Gönderim uygun) ile yanıt verir. CTS paketini alan gönderici verisini hedef düğüme gönderdikten sonra hedef düğümden verinin hatasız alındığını bildiren Alındı (ACK-Acknowledgement) bilgisini bekler. Göndericiye ulaşan ACK mesajı gönderimin başarıyla tamamlandığını ifade eder. RTS/CTS paketlerini alan diğer düğümler ortamı belirtilen gönderim süresi kadar dolu olarak kabul ederler. Mesaj gönderim adımları Şekil 2-2’ de özetlenmiştir:[6]

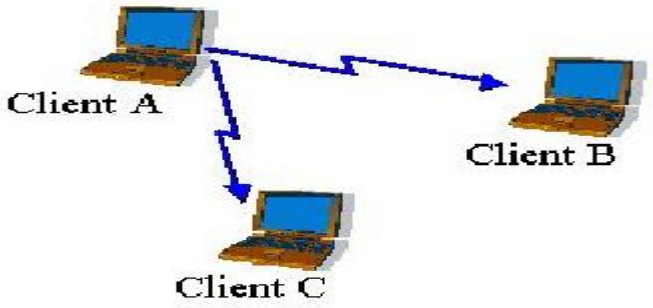


Şekil 2-2: 802.11 Ortam erişimi mekanizması

2.2.3 802.11 Çalışma Mimarileri

802.11 telsiz ağları iki öğeden oluşur; istemciler, örneğin telsiz ağ adaptörü takılı bir bilgisayar ve erişim noktaları. Bu iki öğenin birbirileriyle haberleşmek için oluşturabileceği topolojik yapılar iki çeşittir:

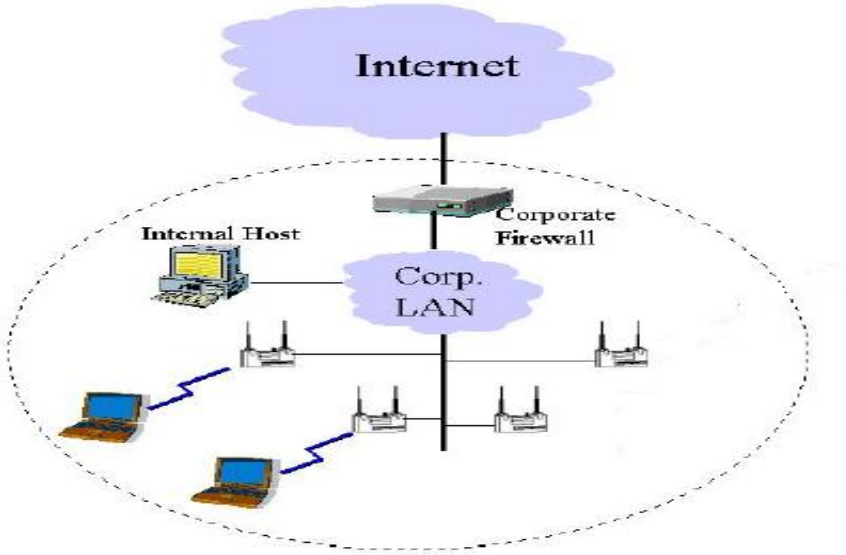
- İstemcilerin herhangi bir erişim noktasına ihtiyaç duymadan kendi aralarında geçici bir ağ oluşturarak haberleşmelerine tasarsız (Ad-hoc) haberleşme topolojisi adı verilir. Şekil 2.3 tasarsız çalışma modunu gösterir:



Şekil 2-3: Tasarsız çalışma modu gösterimi[7]

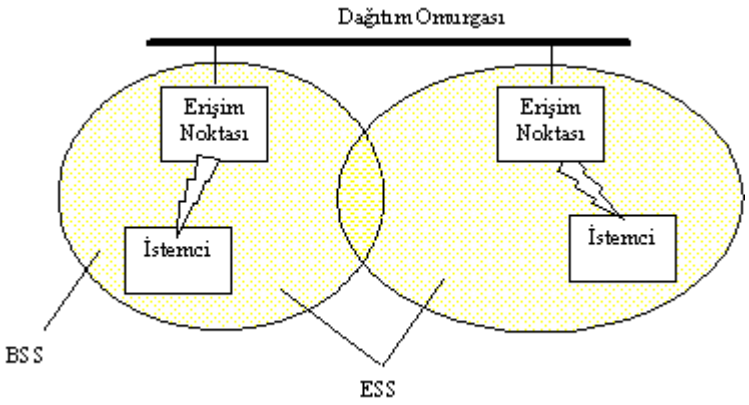
- Genellikle kablolu ağa da bağlı bir erişim noktası ve bu erişim noktası üzerinden gerek birbirleriyle gerekse kablolu ağdaki diğer bilgisayarlarla haberleşen istemcilerin oluşturdukları topolojiye de Altyapılı çalışma

(Infrastructured) modu adı verilir. Şekil 2-4 altyapılı çalışma modunu gösterir:



Şekil 2-4 Altyapılı çalışma modu gösterimi[7]

Her iki topolojide de telsiz ağ temelde hücrelere (cell) bölünmüştür. Tasarsız çalışma modunda tanımlı tek bir hücre vardır ve bu hücreye IBSS (Independent Basic Service Set – Bağımsız temel servis tanımlayıcı) adı verilir. Altyapılı çalışma modunda her hücre bir erişim noktası tarafından yönetilir. Erişim noktalarının yönettikleri her hücreye BSS (Basic Service Set – Temel hizmet tanımlayıcı) adı verilir. Telsiz ağ hücrelere bölünse ve her bir hücre bir telsiz bilgisayar ağı tanımlasa da genellikle telsiz bilgisayar ağı denildiğinde birden fazla hücreye sahip ve hücrelerin yönetiminden sorumlu erişim noktalarının birbirlerine kablolu ağ (örneğin Ethernet) üzerinden bağlandığı yapı akla gelir, bu yapıya ESS (Extended Service Set – Genişletilmiş hizmet tanımlayıcı) adı verilir. Şekil 2-5'de BSS ve ESS şekil olarak gösterilmiştir:[5]



Şekil 2-5: Temel hizmet tanımlayıcı ve genişletilmiş hizmet tanımlayıcı

3 802.11-1999 GÜVENLİK MEKANİZMALARI

IEEE 802.11-1999 telsiz yerel bilgisayar ağları standardında iletişim güvenliği ile ilgili tasarlanan kimlik doğrulama, anahtar yönetimi, veri gizliliği ve bütünlüğünü tanımlayan WEP protokolü 802.11i güvenlik standardıyla geçerliliğini yitirmiş olmasına rağmen 802.11i standardının getirdiği güvenlik mekanizmalarını ve bu mekanizmalara neden ihtiyaç duyulduğunun daha iyi anlaşılması için bu bölümde 802.11-1999 standardı güvenlik mekanizmalarının işleyişi ve zayıflıkları ele alınacaktır.

3.1 Giriş

802.11 telsiz yerel bilgisayar ağları standardının oluşturulması ve bu standardın kullanıcılar tarafından yoğun olarak kullanılmaya başlanmasıyla 2000 senesinin başlarında telsiz bilgisayar ağları güvenlik mekanizmaları, kriptolojik protokol ve algoritmaları inceleyen cemiyetlerin de ilgisini çekmiştir. Kısa bir süre içerisinde standardın tanımladığı tüm güvenlik mekanizmaları kırılmış, 802.11-1999 standardı güvenlik mekanizmalarının güvensiz olduğu anlaşılmıştır. 2001 senesinde 802.11-1999 güvenlik mekanizmalarını delmeyi başaran saldırı programları Internet dünyasında kolaylıkla bulunur hale gelmiştir. Her ne kadar güvensiz olduğu bilinse de telsiz bilgisayar ağları güvenliğinde yeni bir güvenlik standardı oluşturuluncaya kadar 802.11-1999 güvenlik mekanizmaları kullanılmıştır. Aşılması çok zor olmasa da saldırganlar için bir engel oluşturmakta ve “hiç yoktan iyidir” yaklaşımı ile uygulama alanı bulmaktaydı.

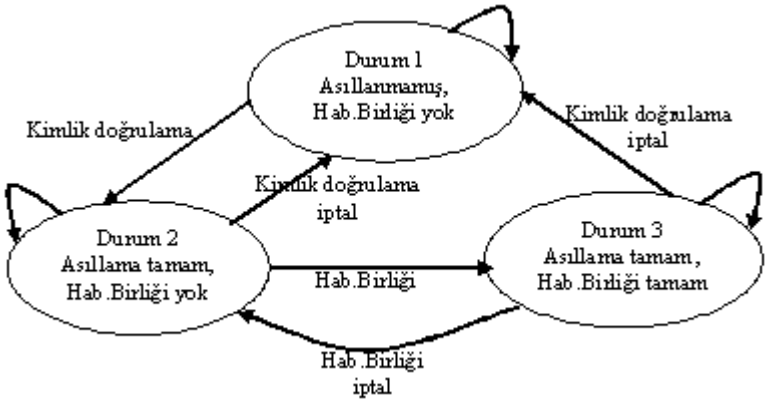
802.11 güvenlik mekanizmalarını tasarlayanlar, güvenlik mekanizmalarını inceleyen camia tarafından; 802.11-1999 güvenlik mekanizmalarını bilinen güvenlik açıklıklarının üzerine inşa etmekle eleştirilseler de güvenlik tasarımı oluşturulurken yapılan kabuller de göz önüne alınmalıdır. 802.11-1999 güvenlik mekanizmaları askeri gizlilik seviyeli verilerin korunması amacıyla tasarlanmamıştır. Adından da anlaşılacağı gibi kablolu eşdeğer gizliliği hedeflemiştir. Örneğin kablolu bir ağa bağlantı kurmak için öncelikle kapıdaki güvenliği geçerek binanın içerisine girmek

gereklidir. Yetkisiz bir kişi için kapıdaki güvenliği geçip içeriye girmek zor fakat imkansız değildir. Benzer şekilde 802.11-1999 güvenlik mekanizmaları aşılması zor fakat imkansız olmayan bir mekanizma kurmayı hedef seçmiştir. 802.11-1999 güvenlik mekanizmaları tasarlanırken yapılan kabulleri inceleyelim[1]:

- Oldukça Güçlü: Protokolün güvenliği, gizli kriptolojik anahtarın kaba yöntemle (brute-force) ortaya çıkarılmasının zor olmasına dayanır. Kriptolojik anahtarın anahtar boyu ve güncellenme sıklığı ve ilklendirme vektörünün rasgele seçilmesi güvenliği doğrudan etkiler.
- Kendinden Senkronize: WEP kapsüllemesi ile güvenliği sağlanarak gönderilen her pakette kriptolojik senkronizasyon kendiliğinden sağlanır. Önceden gönderilmiş paketlerin kaybolması senkronizasyonu bozmaz.
- Verimli çalışır: 802.11-1999 güvenlik mekanizmaları donanım üzerinde gerçeklenebilecek kadar yalın olarak tasarlanmıştır, ayrıca yazılımla da gerçeklenebilir.
- İhraç Edilebilir: 802.11-1999 standardının tasarlandığı dönemde A.B.D. ihraç yasaları güçlü kriptolojik işlemler yapabilen ürünlerin A.B.D. dışına satışına izin vermemekteydi. Tasarlanan güvenlik mekanizmaları yasaların izin vereceği ölçüde kriptolojik işlemler kullanır, bu nedenle 802.11-1999 güvenlik mekanizmalarını kullanan ürünler A.B.D. dışına kolaylıkla ihraç edilebilirler.
- Seçime Bağlıdır: 802.11-1999 standardına göre WEP kapsüllemesinin gerçeklenmesi ve kullanılması zorunlu değil seçimlidir.

Yapılan kabullerin bir kısmının yanlış olduğu zaman içerisinde ortaya çıkmıştır. Örneğin güvenlikten söz edilirken "Oldukça Güçlü" kabulü anlamsızdır. Güvenlik camiası için bir protokol ya güvenlidir ya da güvensizdir, "Oldukça Güçlü" kabulü belirsizlik ifade eder. Güvenliğin anahtar boyu ile ilintili olmadığı yapılan çalışmalarda anlaşılmıştır [8], fakat üreticiler anahtar boyunu uzatarak "daha güvenli" ibaresini ürünlerin üzerine koymaktan çekinmemişlerdir.

802.11-1999 standardında haberleşmeye geçiş aşamaları Şekil 3-1' ile [1] özetlenebilir:



Şekil 3-1: 802.11 İstemci durum makinesi

3.2 Kimlik Doğrulama

802.11 telsiz ağına katılmak isteyen istemci haberleşmeye geçebilmek için öncelikle yetkili bir kullanıcı olduğunu ispatlaması gereklidir. Benzer şekilde istemcinin de kimliğini sorgulayacak öğeyi doğrulayabilir olması gerekir. Bu adıma karşılıklı kimlik doğrulama adı verilir. 802.11-1999 kimlik doğrulama mekanizması olarak iki seçenek tanımlar:

- Açık Sistem: Yetkilendirme isteyen tüm kullanıcılara herhangi bir işlem yapmadan yetki verilir.
- Paylaşılan Anahtar: Paylaşılan gizli anahtarın varlığına dayanır. Sadece gizli anahtarın var olduğunu ispat edebilen istemci yetkilendirilir.

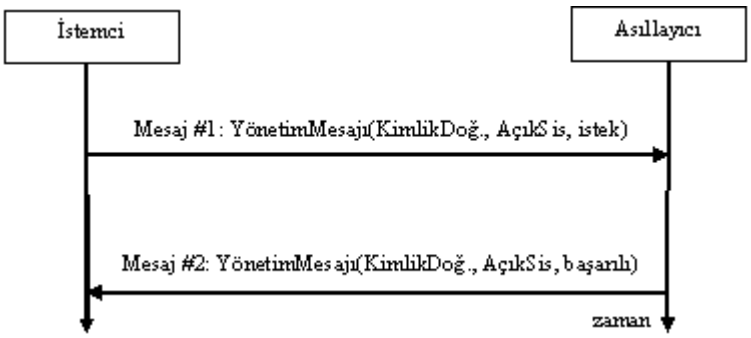
802.11-1999 standardında tanımlı iki yöntem de karşılıklı kimlik doğrulama işleminin amaçlarını yerine getirmekten uzaktır.

Kimlik doğrulama işlemi için gönderilecek mesajlar yönetim mesajları tipinden mesajlardır ve uçtan-uca gönderilir, çoğa-gönderim kimlik doğrulama oluşturmak için gönderilecek mesajlarda geçerli değildir. Kimlik doğrulama iptalini belirten mesajlar bildiri şeklinde olduğundan grup adresine gönderilebilir.

3.2.1 Açık Sistem Kimlik Doğrulama:

802.11-1999 standardında ön tanımlı kimlik doğrulama metodu açık sistemdir. Yetkilendirme isteyen tüm kullanıcılara herhangi bir işlem uygulanmadan yetki verilir. Açık sistem kimlik doğrulama işlemi 2 mesajın gönderilip alınmasıyla tamamlanır, mesajlara herhangi bir veri bütünlüğü sınaması veya şifreleme

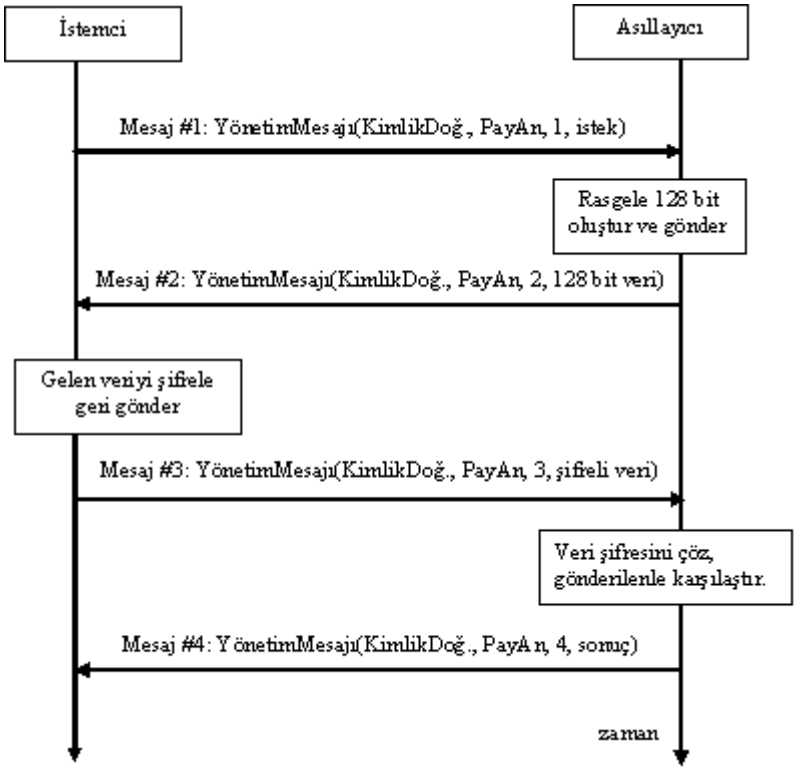
uygulanmaz. Şekil 3-2'de açık sistem kimlik doğrulamaya ilişkin mesaj alış-verişleri verilmiştir:



Şekil 3-2: Açık sistem kimlik doğrulama mesaj alış-verişi

3.2.2 Paylaşılan Anahtarla Kimlik Doğrulama

Paylaşılan gizli anahtarın varlığına dayanır, sadece gizli anahtarın var olduğunu ispat edebilen istemci yetkilendirilir. Gizli anahtar daha önceden 802.11 ağı dışında güvenli bir mekanizmayla karşılıklı taraflara yüklenmiş olmalıdır. WEP şifreleme mekanizmasını kullanır. Yeni bir istemci yetkilendirme isteğinde bulunduğunda asıllayıcı 128 bitlik rasgele bir sayı hazırlayarak istemciye gönderir. İstemci alacağı bu 128 bitlik sayıyı şifreleyerek asıllayıcıya geri gönderir. Asıllayıcı istemciden aldığı şifreli mesajı çözdüğünde kendi gönderdiği 128 bitlik sayıyı bulabiliyorsa istemcinin doğru anahtara sahip olduğunu dolayısıyla yetkilendirilmiş olduğunu anlar ve istemciye kimlik doğrulama işleminin sonucunun başarılı olduğunu bildirir. Kendi gönderdiği sayıyı bulamaz ise istemcinin gerekli olan gizli anahtarı bilmediği sonucuna varır ve istemciye kimlik doğrulama başarısız durumunu iletir. Toplam 4 mesaj gönderilip alınır. Şekil 3-3'de paylaşılan anahtarla kimlik doğrulamaya ilişkin mesaj alış-verişleri verilmiştir.



Şekil 3-3: Paylaşılan anahtarla kimlik doğrulama

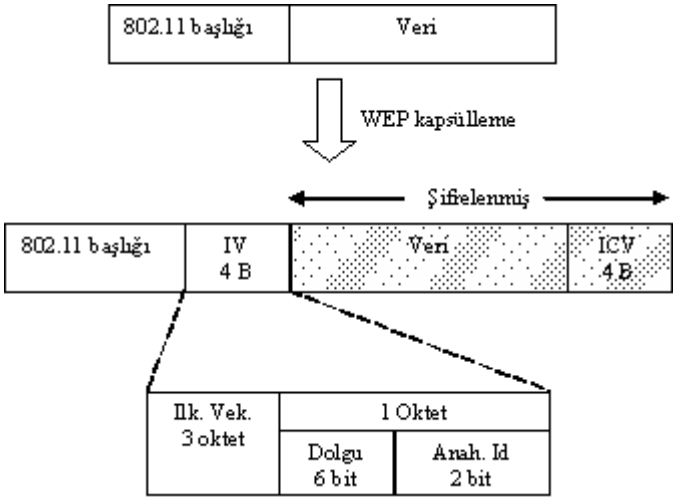
3.3 WEP

Veri gizliliğinin sağlanması amacıyla tasarlanmıştır. İstenmeyen kişilerin mesajları yakalayıp anlamalarını engellemeyi hedefler, RC4 şifreleme algoritmasını kullanır. WEP' in gerçeklenmesi ve kullanılması 802.11-1999 standardına göre seçime bağlıdır. Anahtar boyu standartta 40 bit olarak tanımlanmıştır, fakat uygulamada üreticiler anahtar boyunu 104 bite de çıkarmışlardır. WEP-40 anahtar boyunun 40 bit ve WEP-104 anahtar boyunun 104 bit olmasını ifade eder. Her iki anahtar boyu içinde yapılan işlemler aynıdır. Anahtar boyunun 104 bite yükseltilmesi daha güvenli anlamını taşımamaktadır [8].

WEP kapsülleme gönderilecek her paket için ayrı yapılır.

3.3.1 WEP paketi yapısı

Kapsülleme işlemi bölmelemeden sonra, paket yola çıkartılmadan önce gerçekleştirilir. Kapsülleme işlemi paket boyunu 8 sekizli arttırır, bu nedenle bölmeleme yapılacaksa WEP kapsülleme uygulanıp uygulanmayacağı göz önünde bulundurulmalıdır. Şekil 3-4'de kapsüllemenin gönderilecek paket üzerinde yapacağı değişiklikleri görebiliriz:



Şekil 3-4: WEP uygulanması sonrası paket yapısındaki değişiklikler

3.3.2 Bütünlük Sınaması

Bütünlük sınaması kontrolünün (ICV-Integrity Check Value) amacı mesajın yolda herhangi biri tarafından değiştirilip değiştirilmediğini anlamaktır. Bu amaçla genellikle kriptolojik özet fonksiyonları kullanılırken 802.11' de basit olması sebebiyle CRC-32 (CRC-Cyclic Redundancy Check) kullanılmıştır.

Bütünlük sınaması kontrolü şifrelenmemiş veri üzerinden 32 bitlik Çevrimli Fazlalık Sınaması (CRC) olacak şekilde hesaplanır ve şifrelenmemiş verinin sonuna eklenir. CRC üreteç polinomu aşağıda verilmiştir:

$G(x): x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

3.3.3 WEP IV

Şifreleme amaçlı kullanılan anahtarın tüm paketler için aynı olması beraberinde bir problem de taşır. Belli aralıklarla anahtar güncellense de anahtar güncellemeleri arasında anahtar sabit kalır ve şifrelenecek tüm veriler aynı anahtar kullanılarak şifrelenir. Bu durumda aynı giriş için şifreleme algoritması sürekli aynı çıkışı üretecektir. Örneğin "abcdef" dizisinin RC4 algoritmasıyla şifrelendiğinde "t*fPr%" çıktısını ürettiğini kabul edersek anahtar güncellenmediği sürece her "abcdef" dizisinin şifrelenmesinde aynı çıktı elde edilir.

Genellikle haberleşmede TCP/IP protokol kümesinin kullanıldığı ve IP başlığındaki alt alanların sürekli aynı yere yazıldığı düşünüldüğünde aynı anahtarla şifrelendiğinde sürekli aynı çıktılar elde edilir. Bu durum saldırganın gönderilen

şifreli verileri analiz ederek zaman içerisinde gizli anahtarı elde etmesiyle sonuçlanabilir.

Yukarıda ifade edilen problem aynı anahtarla şifrelese de her şifreleme işleminde farklı olacak başka bir değerin şifreleme işlemine katılmasıyla çözülebilir. Şifreleme işleminde kullanılan ve aynı anahtarla yapılan her şifreleme işleminde farklı olan değere İlklendirme Vektörü (IV) adı verilir.

IEEE 802.11-1999 standardında tanımlanan IV' nin boyu 24 bit yani üç sekizlidir. Her şifreleme işleminde kullanılan IV değeri, paketi alacak tarafın şifreyi çözebilmesi için paketin içine açık bir biçimde yazılır. IV' nin bilinmesi gizli anahtarın bilinmediği durumda hiç bir anlam ifade etmez. Burada dikkat edilmesi gereken durum ise aynı IV değerinin aynı anahtar için birden fazla kere kullanılmamasıdır. IV alanının 24 bit olması 2^{24} = 16.777.216 farklı IV değerinin olabileceğini gösterir. Oldukça yüksek görünse de ortalama yoğunluktaki 11 Mbps kapasiteli erişim noktasının saniyede 700 paket gönderdiği düşünüldüğünde IV alanı 7 saat içerisinde tüketilecektir. IV alanı tüketildikten sonra anahtar değişimi yapılmaması durumunda aynı anahtar ve IV ile şifrelenecek paketler gönderilmeye başlanacak, bu durumda sürekli hattı dinleyecek saldırgan yapacağı analizler sonucunda gizli anahtarı elde edebilecektir.

Aynı IV değerinin kullanılmaya başlanması için 7 saat geçmesi de gerekmeyebilir. Bir çok gerçeklemede cihazlar ilk açıldıklarında IV değeri sıfırdan başlatılarak birer artırılarak seçilir. Bu durumda haberleşmeye katılan her yeni cihaz başta aynı anahtar ve IV değeri ile şifrelemeye başlayacaktır. Aynı anahtar ve IV ile şifrelenmiş birden fazla veri paketi olmuş olacaktır.

IV değerinin rasgele seçilmesi IV yeniden kullanımını engelleyemeyecektir. Doğum-günü paradoksu adı verilen olasılık hesabına göre IV değerleri rasgele seçilse de ortalama 5000 paket içerisinde [9] aynı IV değerini kullanmış birden fazla şifreli paket bulmak mümkündür.

3.3.4 RC4 Algoritması

Güvenlik mekanizmalarında kullanılan şifreleme yöntemleri akış şifreleme ve blok şifreleme olarak ikiye ayrılabilir. Akış şifreleme yönteminde şifreleme algoritması açık veriyi sekizliler halinde alarak aldıkları her sekizliye karşılık şifrelenmiş bir sekizli (kriptolojik yöntemlerle karıştırılmış) üretirler. Blok şifreleme yönteminde ise

şifrelenecek açık veri, algoritmanın gerektirdiği uzunlukta bloklara (örneğin 8,16, 32 sekizli) ayrılarak algoritma sonucunda şifrelenmiş (kriptolojik yöntemlerle karıştırılmış) yeni bloklar üretirler. Akış şifrelemede algoritmanın dahili durumu her sekizlide güncellenirken blok şifrelemede her yeni bloğu şifrelemek için algoritma dahili durumu ilk haline geri alınır.

WEP algoritması veri şifreleme işlemleri için RC4 akış şifreleme algoritmasını kullanır. RC4[1] algoritması "RSA Güvenlik" firmasının bir ürünüdür ve 802.11 WEP gerçeklemesi için bu firmadan istenebilir. Şifreleme işlemi için IV ve gizli anahtar kullanılarak ilklendirilen RC4-PRNG (PRNG – Pseudo Random Number Generator, Sözde Rasgele Sayı Üreteci)' den anahtar dizisi üretilir ve üretilen bu anahtar dizisi ile açık veri dışlamalı veya (XOR-Exclusive OR) işlemi ile şifreli veri oluşturulur. Şifreleme işlemi sembolik olarak aşağıda verildiği şekilde gösterilebilir:

$$C = P \oplus RC4(V,K)$$

C: Şifreli veri (cipher text) ifade eder.

P: Açık veriyi (plain text) ifade eder.

V: İlklendirme Vektörünü (IV) ifade eder.

K: Gizli anahtarı (key) ifade eder.

$\oplus$: Dışlamalı veya (XOR) işlemini ifade eder.

RC4(a, b): RC4-PRNG işlemini ifade eder.

Şifre çözme işleminde, uygulanan işlemler tersten uygulanarak açık veri elde edilir. Bu amaçla gerekli olan gizli anahtar şifre çözme işlemini gerçekleştirecek istemcide önceden yüklü olmalıdır. İşlem sırasında kullanılacak IV değeri şifreli paketin içerisine açık olarak yazıldığından buradan okunabilir:

$$P' = C \oplus RC4(v,k)$$

$$P' = (P \oplus RC4(v, k)) \oplus RC4(v, k)$$

$$P' = P \oplus (RC4(v,k) \oplus RC4(v, k))$$

$$P' = P \oplus 0$$

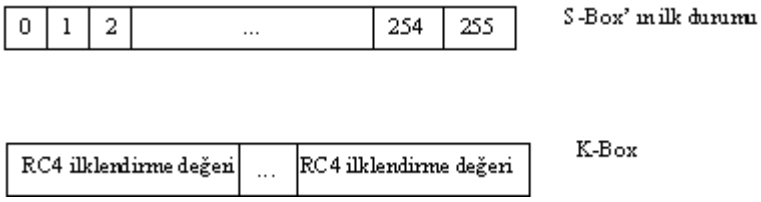
$$P' = P$$

[1] RC4, Ron Rivest tarafından geliştirilen 4. şifreleme algoritmasıdır(RC4 -Rivest Cipher 4).

RC4 algoritmasının iki aşaması vardır:

- Anahtar çizelgesinin oluşturulması (değişim kutusunun oluşturulması)
- Rasgele sekizli dizisinin oluşturulması

Anahtar çizelgesi 0-255 arası sayıları barındıran sekizli dizisidir. Anahtar çizelgesini oluşturmak için öncelikle 0' dan 255' e kadar olan sayılar sırayla bir diziye yazılır, bu diziye değişim kutusu S-Box adı verilir. 256 sekizlilik K-Box adı verilen ikinci bir sekizli dizisi ilklendirme değeri ile doldurulur. İlklendirme değerinin 256 sekizliden küçük olması durumunda, örneğin WEP-104 için 16 defa, 256 sekizli doldurulunca kadar ardı ardına ilklendirme değeri diziye yazılır. S-Box ve K-Box' ların ilk durumları Şekil3-5'de verilmiştir:



Şekil 3-5: RC4 yer değiştirme kutularının ilk durumları

S-Box' ın oluşturulması için S-Box' taki her bir sayı yine S-Box' taki başka bir sayıyla yer değiştirilir. Yer değiştirme işlemi için tanımlı algoritma aşağıdaki gibidir:

byte i = j = 0;

for i = 0 to 255 do

j = (j + S-Box[i] + K-Box[i]) (mod 256)

Swap S-Box[i] and S-Box[j]

End

Yürütülecek bu algoritmanın sonunda 0-255 değerleri S-Box içerisinde rasgele bir sırayla yer alacaktır. Bir sonraki adım rasgele sekizli dizisinin oluşturulmasıdır. Rasgele sekizlilerin oluşturulması için kullanılan algoritma aşağıda verildiği gibidir:

i = (i + 1) (mod 256)

j = (j + S-Box[i]) (mod 256)

Swap S-Box[i] and S-Box[j]

k = (S-Box[i] + S-Box[j]) (mod 256)

R = S-Box[k]

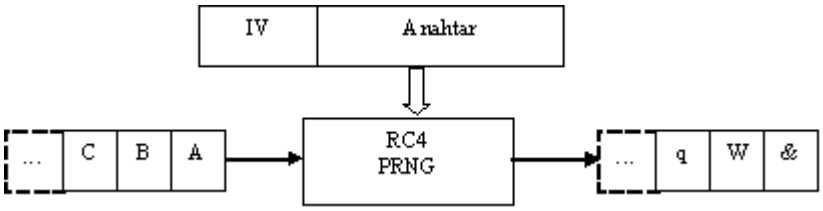
R değeri her bir ötelemede elde edilen rasgele sekizli değerini ifade eder. Şifreleme işlemi için elde edilen rasgele sekizli değeri (R) ötelemedeki açık veri sekizlisi ile dışlamalı veya işleminden geçirilir. Öteleme açık verideki tüm sekizliler tüketilinceye kadar devam ettirilir.

3.3.5 RC4 ilklendirme değerinin oluşturulması

Şifreleme ve şifre çözme işlemlerinde kullanılan RC4-PRNG' yi ilklendirmek (WEP seed) için ilklendirme vektörü ve gizli anahtar kullanılır. IV her paket için değiştiğinden her pakette yeniden oluşturulur. Yapılan işlem aslında IV değerinin sonuna anahtarı eklemektir:

WEP-seed = [IV || Anahtar]

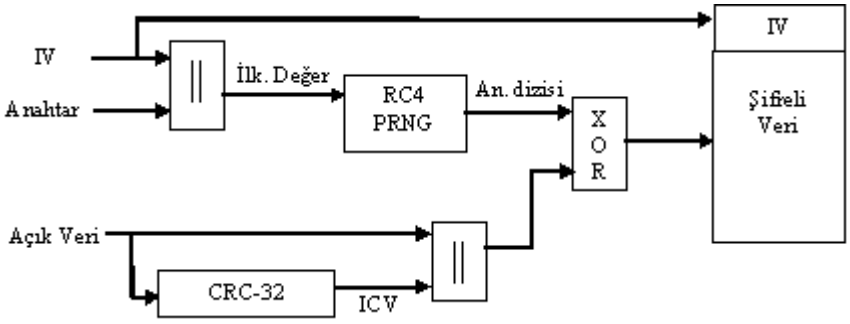
IV değeri 24 bit, WEP-40 için anahtar boyu 40 bit, WEP-104 için anahtar boyu 104 bittir. Sonuç olarak oluşturulacak RC4 ilklendirme değeri 64 bitlik (WEP-40 için) veya 128 bitlik (WEP-104 için) bir değer olacaktır. Şekil 3-6 RC4 şifreleme işlemini şekil olarak göstermektedir.



Şekil 3-6: RC4 Şifreleme

3.3.6 WEP Şifreleme

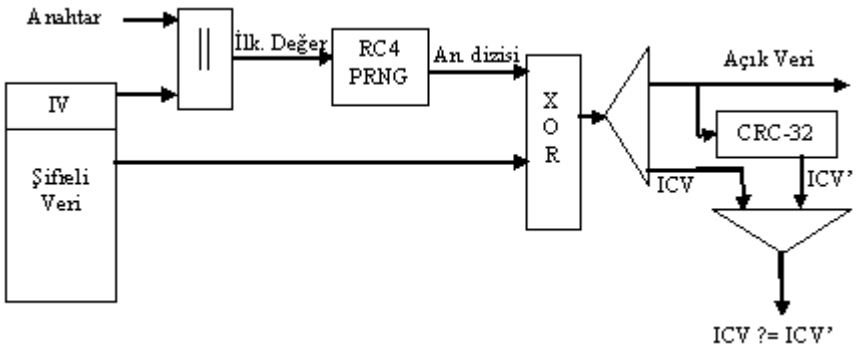
WEP kapsüllemenin yapılması için paket üzerinde 3 işlem gerçekleştirilir. İlk olarak bütünlük sınaması değeri açık veri üzerinden CRC-32 kullanılarak hesaplanır ve elde edilen değer açık verinin sonuna eklenir. Daha sonra IV ve anahtar değerleri kullanılarak RC4 ilklendirme değeri üretilir ve bu değer kullanılarak açık veri ve bütünlük sınaması değeri RC4 akış şifreleme işleminden geçirilir. Son olarak kullanılan IV değeri ve anahtarın kimliği alıcı tarafın paketi doğru olarak çözebilmesi için pakete açık olarak işlenir. Yapılan işlemler Şekil 3-7'de gösterilmiştir:



Şekil 3-7: WEP Şifreleme mekanizması

3.3.7 WEP Şifre Çözme

Alınan şifreli verinin çözülerek açık verinin elde edilmesi için 3 işlemin uygulanması gereklidir. Öncelikle (gönderici, alıcı) çifti için bir anahtar tanımlandıysa ilgili anahtar alıcı tarafından bulunur. Eğer (gönderici, alıcı) çifti için bir anahtar tanımlanmamışsa şifreli paketin içerisinden anahtar kimlik numarası okunur ve paketin şifrelendiği anahtar bulunur. İkinci işlem olarak elde edilen anahtar ve paketten okunan IV ile RC4 ilklendirme değeri oluşturulur ve paket içerisindeki şifreli veri çözülür. Son olarak açık veri üzerinden bütünlük sınaması CRC-32 kullanılarak tekrar hesaplanır ve paket içerisinde bulunan ve göndericinin hesaplamış olduğu bütünlük sınaması değeri ile karşılaştırılır. Hesaplanan bütünlük sınaması değeri ile paketin içerisinde yer alan bütünlük sınaması değerleri aynıysa paket işlenmek üzere üst katmanlara iletilir, aksi durumda paket başka bir işlem yapılmadan atılır. Yapılan işlemler Şekil 3-8'de gösterilmiştir:



Şekil 3-8: WEP Şifre çözme mekanizması

3.3.8 WEP Anahtarları

IEEE 802.11-1999 standardında, tanımlı güvenlik mekanizmalarında (asıllama ve şifreleme) kullanılacak kriptolojik anahtarların açık bir tanımı yapılmamıştır. Üreticiler farklı isimler altında farklı anahtarlar tanımlamış ve kullanmışlardır. Örneğin bazı üreticiler standartta tanımlı 4 anahtardan oluşan WEP anahtarına paylaşılan anahtar adını verirken bazıları da bu anahtarları çoğa gönderim anahtarı olarak isimlendirmiş ve kullanmışlardır. IEEE 802.11-1999 standardında tanımlı iki anahtar tipi söz konusudur:

- Varsayılan anahtarlar
- (Gönderici, Alıcı) çifti anahtarları

İster varsayılan anahtar olsun ister (gönderici, alıcı) çifti için tanımlı anahtar olsun, her iki tip anahtarın da ortak özellikleri şunlarıdır:

- Paylaşılan Anahtarlardır: Varsayılan anahtarlar ortamda bulunan ve haberleşmeye katılacak tüm istemci ve erişim noktalarında aynı olan anahtarlardır. (Gönderici, alıcı) çifti için tanımlı anahtarlar sadece gönderici ve alıcıda tanımlı olsalar da yine her iki uç tarafından paylaşılırlar.
- Simetrik Anahtarlardır: Şifre çözme işlemi ancak ve ancak şifrelemenin yapıldığı anahtarla yapılabilir.
- Statik Anahtarlardır: Sistem yöneticisi tarafından güncellenmediği sürece tanımlı tüm anahtarlar değiştirilmeksizin kullanılırlar. 802.11-1999 standardında otomatik anahtar güncelleme mekanizması tanımlı değildir.
- Uzunlukları Sabittir: WEP-40 kullanıldığında 40bit, WEP-104 kullanıldığında 104 bit olacak şekilde anahtarların boyu sabittir.

Varsayılan anahtarlar toplam dört tanedir. Haberleşmeye katılacak tüm istemci ve erişim noktalarında aynı olacak şekilde ayarlanmalıdırlar. Teke gönderim paketlerinin şifrelenmesinde kullanılabileceği gibi çoğa gönderim paketlerinin şifrelenmesinde de kullanılırlar. Şifreleme ve şifre çözme işlemleri için tek anahtarın tanımlı olması yeterli olsa da anahtar değiştirme işlemlerinin sorunsuzca gerçekleştirilebilmesi için 4 anahtar tanımlanmıştır. WEP şifrelemesinde bu 4 anahtardan biri kullanılacaksa anahtarın indis numarası paket başlığına yazılır, böyle alıcı tarafta tanımlı 4 anahtardan hangisi ile şifre çözme işlemini gerçekleştirmesi

gerektiğini bilebilir. Varsayılan anahtarlar her istemcide aynı olacağından bir istemciye gönderilmiş şifreli bir mesaj istenirse başka bir istemci tarafından okunabilir. Bu nedenle teke gönderim mesajlarının (gönderici, alıcı) çifti için tanımlı anahtarla şifrelenmesi daha uygun olacaktır.

(Gönderici, alıcı) çifti için tanımlı olan anahtarlar sadece tanımlı olduğu gönderici ve alıcı tarafından paylaşılır. Erişim noktası bir istemciye şifreli bir paket göndereceğinde bu istemci için bu şekilde bir anahtar tanımlandıysa varsayılan anahtarlar yerine bu anahtarı kullanır. Alıcı tarafta da paket başlığında yazan varsayılan anahtar numarası dikkate alınmaksızın (gönderici, alıcı) için tanımlanmış anahtarı şifre çözme işleminde kullanılır. 802.11 alt yapılı çalışma modunda her bir istemci için ayrı bir (gönderici, alıcı) çifti anahtarı tanımlanması durumunda erişim noktası her bir istemci için ayrı bir şifreleme anahtarı tutacaktır. Bu durumda hiç bir istemci diğerine adreslenmiş şifreli bir paketin içeriğini çözemez. Çoğa gönderim söz konusu olduğunda (gönderici, alıcı) çifti anahtarları kullanışsız olacaktır. Çoğa gönderim mesajlarının şifrelenmesinde tüm istemcilerde bulunacak varsayılan anahtarlar kullanılmalıdır.

3.4 802.11-1999 standardı Güvenlik Zayıflıkları

802.11 telsiz yerel bilgisayar ağları standardının oluşturulması ve bu standardın kullanıcılar tarafından yoğun olarak kullanılmaya başlanmasıyla araştırmacıların da ilgisini çekmiş, yapılan araştırmalar sonucunda tanımlanmış güvenlik mekanizmaların hemen hepsinde problemler olduğu ortaya çıkartılmıştır [7, 8, 9]. Bu bölümde 802.11-1999 standardındaki güvenlik mekanizmalarının zayıflıkları ele alınacaktır.

3.4.1 Asıllama Zayıflıkları

Asıllama işlemi ağ kaynaklarını kullanmak isteyen kullanıcıların gerçekten iddia ettikleri kişi olup olmadıklarını ve ağ kaynaklarını kullanmaya yetkili olup olmadıklarının ispat edilmesidir. 802.11-1999 standardı tanımladığı yöntemlerle karşılıklı asıllamanın gerçekleştirilebileceğini savunur. 802.11-1999 standardında tanımlı iki asıllama metodu mevcuttur, açık sistem asıllama, paylaşılan anahtar kullanılarak asıllama.

Açık sistem asıllama da istekte bulunan her kullanıcı her hangi bir işleme tabi tutulmaksızın yetkilendirilir. Karşılıklı kimlik doğrulama gerçekleştirilmemiştir. Paylaşılan anahtarla asıllama işleminde istekte bulunan kullanıcıya erişim noktası rasgele 128 sekizlilik bir sayı gönderir, kullanıcı bu sayıyı kendisinde mevcut anahtarla şifreleyerek erişim noktasına geri gönderir. Erişim noktası gelen şifreli mesajı çözdüğünde kendi göndermiş olduğu 128 sekizlilik sayıyı bulabilirse kullanıcının şifreleme işlemi için geçerli bir anahtara sahip olduğu dolayısıyla ağ kaynaklarını kullanmaya yetkili olduğu sonucuna varır. Bu işlemde erişim noktasının kullanıcıyı anahtarın varlığını kontrol ederek asılladığı fakat kullanıcının erişim noktasını asıllamadığı açıktır, yani karşılıklı kimlik doğrulama gerçekleştirilmemiştir. Dahası paylaşılan anahtarla kimlik doğrulama adımlarını takip eden yetkisiz bir saldırgan gizli anahtarı bilmese de asıllama işlemini başarıyla gerçekleştirebilir [7, 9]. Paylaşılan anahtarla kimlik doğrulama işleminin ikinci adımında erişim noktası kullanıcıya şifresiz olarak 128 sekizlilik rasgele bir sayı gönderir, bu sayıya P diyelim. İstemci bu sayıyı kendisinde bulunan anahtarla şifreleyerek erişim noktasına gönderir, şifreli bu veriye C diyelim. WEP şifreleme mekanizması hatırlanacak olunursa öncelikle IV ve anahtar kullanılarak bir anahtar dizisi oluşturuluyor ve bu anahtar dizisi şifrelenecek veriyle dışlamalı veya (xor) işlemine tabi tutuluyordu, bu anahtar dizisine K diyelim:

$$C = P \oplus K$$

Paylaşılan anahtarla kimlik doğrulama işlemi adımlarını takip eden bir saldırgan P ve C bilgilerini ağı dinleyerek edinir. Elde ettiği bu verileri dışlamalı veya işlemine tabi tuttuğunda, istemci tarafından IV ve anahtar kullanılarak oluşturulmuş anahtar dizisini (K) elde eder:

$$P \oplus C = P \oplus (P \oplus K) = (P \oplus P) \oplus K = (0) \oplus K = K$$

Daha sonra saldırgan erişim noktasından asıllama isteğinde bulunur. Kendisine gönderilen rasgele 128 sekizlilik veriyi elde etmiş olduğu K anahtar dizisini kullanarak dışlamalı veya işleminden geçirir ve şifreli veriyi elde etmiş olur. Erişim noktasına göndereceği mesajda IV olarak bir önceki istemciden elde ettiği IV değerini aynen kullanarak erişim noktasının da aynı K anahtar dizisini oluşturmasını ve mesajı doğru çözmesini sağlamış olur. Böyle paylaşılan gizli anahtara sahip olmadan asıllama işlemini gerçekleştirir.

Sonuç olarak paylaşılan anahtarla asıllama işlemi karşılıklı asıllamayı gerçekleştirmediği gibi takip edilen geçerli bir asıllama işlemi sonucunda saldırganlara asıllama için gerekli tüm bilgileri vermiş olur. Güvenlik protokollerinde genel kabul olan asıllama işlemlerinde kullanılacak anahtarlar ile gönderilen verinin şifrelenmesinde kullanılacak anahtarların farklı olması gerektiği kabulü de kullanılmadığından, daha da kötü olarak doğrudan anahtarın ele geçirilmesi için yapılacak saldırılara da veri sağlar. Doğrudan gizli anahtarın ortaya çıkarılması için yapılacak saldırılarda açık veri ve anahtarla şifrelenmiş halleri analiz edilerek anahtar elde edilmeye çalışılır. Paylaşılan anahtarla asıllama işlemi doğrudan anahtar saldırıları için gerekli olan açık veri ve şifrelenmiş hali için 128 sekizlilik bir bilgi sağlamış olur.

3.4.2 Erişim Kontrolü Zayıflıkları

Asıllama işlemi istemcinin olduğunu iddia ettiği kişi olup olmadığını ispat etmeye yönelik olmalıdır. Kişinin gerçekte olması gereken kişi olduğunu ispat etmesi ile ağ kaynaklarına erişimine yetkisi olması arasında fark olmalıdır. 802.11-1999 standardı bu iki kavramı birlikte kullanır ve erişim denetimi için başka bir mekanizma tanımlamaz.

Üreticiler ise istemcilerin MAC adreslerine dayalı bir erişim kontrolü mekanizması eklemişlerdir. Bu mekanizmaya göre her bir erişim noktasında ağ kaynaklarını kullanmaya yetkili istemcilerin MAC adresleri bir liste halinde tutulur ve erişim izni isteyen her kullanıcının öncelikle bu listede varlığı sorgulanır. Fakat MAC adreslerine dayalı bir erişim denetimi adreslerin taklit edilebilir olduğu bilgisi altında gerçek bir güvenlik ve erişim denetimi sağlamaktan uzaktır [10].

Erişim noktaları normalde belirli aralıklarla kendilerini tanıtan birer tanıtım paketi yayınlarlar. Bazı üreticiler erişim noktalarının bu yayınlarını kapatarak sadece erişim noktası bilgilerini önceden bilen kullanıcıların ağa erişebileceğini ve erişim denetiminin sağlanabileceğini düşünmüşler ve bu uygulamaya kapalı ağ erişimi (Closed Network Access) adını vermişledir. Erişim noktalarının tanıtım mesajları yayınlaması engellense de bu bilgilere daha önceden sahip olan kullanıcıların ağa erişmek istemeleri sırasında kullanılacak yönetim mesajları içerisinde ağ ile ilgili bilgiler açık olarak taşınır. Böyle bir durumda mevcut erişim noktaları hakkında bilgi sahibi olmayan bir saldırgan sadece pasif olarak ortamı dinleyerek mevcut ağlar

hakkında bilmesi gereken tüm bilgilere erişebilir. Üreticiler tarafından önerilen ve kullanılan kapalı ağ erişimi mekanizması erişim denetimini sağlamaktan uzaktır.

3.4.3 Paket Tekrarı Saldırıları

WEP protokolünde paket tekrarı saldırılarının engellenmesini sağlayacak bir mekanizma kullanılmamıştır. Bir saldırganın yeni açılan bir istemcinin haberleşmesini izlediğini varsayalım. İstemci ilk etapta erişim isteyeceği sunucuya kullanıcı adı ve parola gönderecektir. Kullanıcı adı ve parola şifreli olarak gönderilseler bile haberleşmeyi izleyen ve hangi adımların gerçekleştirilmesi gerektiğini kabaca tahmin eden saldırgan istemcinin bu paketlerini yakalayarak aynen tekrarlaması sonucunda kullanıcı adı ve parolayı bilmeden sunucuya erişim yetkisini elde edebilir. Başka bir örnek olarak telsiz ağ haberleşmesiyle bir banka hesabından para transferi yapıldığını varsayalım. Saldırgan para transferi mesajlarını yakalayıp tekrarlayarak aktarılan paraların miktarlarında değişiklik yapabilir.

802.11 mesajları için başlık alanında sıra numarası verilse bile bu alan WEP ile herhangi bir şekilde korunmadığından güvenlik sağlayıcı bir mekanizma oluşturmaz. Paket tekrarı saldırıları aynı zamanda başka saldırılar için zemin hazırlayıcı saldırılar olarak da kullanılabilir.

3.4.4 Veri Bütünlüğü Zayıflıkları

Bütünlük sınaması kontrolünün (ICV-Integrity Check Value) amacı mesajın yolda herhangi biri tarafından değiştirilip değiştirilmediğini anlamaktır. Bu amaçla 802.11-1999 standardında CRC-32 kullanılmıştır. Bütünlük sınaması kontrolü şifrelenmemiş veri üzerinden 32 bitlik Çevrimli Fazlalık Sınaması (CRC) olacak şekilde hesaplanır ve şifrelenmemiş verinin sonuna eklenir. Şifreli mesajda değişiklik yapıldığında şifre çözme işlemi sonucunda elde edilecek bütünlük sınaması değerinin mesajın içindeki değerle tutmayacağından mesajın değiştirildiğinin anlaşılacağı varsayılmıştır.

CRC-32 fonksiyonu lineer bir fonksiyondur. Yani mesajda herhangi bir bitin değiştirilmesi sonucunda ICV değerinde hangi bitlerin değiştirilmesiyle ICV değerinin tekrar doğru olarak hesaplanacağı önceden bilinebilir. Ayrıca CRC değeri hesaplanırken bütünlük kontrolü için kullanılabilecek bir mesaj bütünlüğü anahtarı da kullanılmaz.

Örneğin IP başlığı sabit uzunluktadır ve alt alanlarının alacağı değerler ve bulunacakları yerler bilinebilir. Bu durumda saldırgan gönderilen şifreli bir mesajın

hedef IP adresi değerini ve ICV alanındaki uygun bitleri değiştirerek mesajın çözüldükten sonra kendi belirleyeceği bir adrese yönlendirebilir [9]. Gizli anahtar bilinmemesine karşın mesaj erişim noktasında çözüldükten sonra saldırganın belirlediği adrese iletileceğinden mesajın içeriğini kolayca okunabilir. Böylece doğrudan anahtar saldırıları için gerekli olan şifreli veri ve onun açık hali bilgilerine de ulaşmış olur.

3.4.5 Veri Gizliliği Zayıflıkları

Asıllama, erişim kontrolü eksikliği, veri bütünlüğünün korunamaması başlı başına büyük güvenlik açıklıklarıdır. Fakat saldırganın asıl hedefi gönderilen mesajları değiştirmek, paket tekrarlamaktan ziyade ağa doğrudan erişim sağlayabilmek veya izlediği mesajların içeriğini okuyabilmektir. Bu amaçla ya verileri önceki anlattığımız şekilde bit değiştirmeleri yöntemiyle başka adreslere yönlendirecek ya da doğrudan anahtarı ele geçirmesi gerekecektir. Doğrudan anahtarı ele geçirmek saldırgan için ana hedeftir. WEP anahtarlarını ele geçirilmesi saldırgan için sunucu şifrelerinin de bilinmesi veya tüm sistemleri kullanabileceği anlamını taşımamakla birlikte saldırının devam ettirilebilmesi için gereklidir. Gizli anahtarın bilinmesi durumunda bit değiştirme yöntemiyle mesajın başka adreslere yönlendirilmesine de gerek kalmayacak saldırgan doğrudan sahip olduğu anahtarı kullanarak mesajları okuyabilecektir.

RC4 algoritması ve bu algoritmanın WEP mekanizmasında yanlış kullanılmasından kaynaklanan sorunlar nedeniyle şifreli mesajların okunabilmesi mümkündür. Doğrudan anahtarın ele geçirilmesiyle sonuçlanan bu saldırılar 3 alt kategoriye ayrılarak ele alınmıştır.

3.4.5.1 Anahtar Dizisi Tekrar Kullanımından Kaynaklanan Sorunlar

Açık verinin şifrelenmesi için öncelikle açık veriyle aynı boyda rasgele anahtar dizisi oluşturulur. Anahtar dizisinin oluşturulması aşamaları RC4 algoritmasının ele alındığı bölümde incelenmiştir, kısaca değinecek olursak her paket için üretilen IV değeri gizli anahtarın başına eklenerek bir ilklendirme değeri oluşturulur ve RC4-PRNG ve ilklendirme değeri kullanılarak rasgele sekizli dizisi (anahtar dizisi) oluşturulur. Aynı anahtar için tekrar aynı IV değerinin kullanılması demek RC4 ilklendirme değerinin aynı olması sonuç olarak rasgele oluşturulması gereken anahtar

dizisinin aynı olması demek olacaktır. Aynı IV değeri ile şifrelenmiş iki mesajı ele alalım:

$C_1 = P_1 \oplus K$ ve $C_2 = P_2 \oplus K$

Şifreli bu iki mesajı birbiri ile dışlamalı veya işlemine tabi tutarsak:

$C_1 \oplus C_2 = (P_1 \oplus K) \oplus (P_2 \oplus K) = (P_1 \oplus P_2) \oplus (K \oplus K)$

$C_1 \oplus C_2 = P_1 \oplus P_2$ elde ederiz.

Saldırganın açık mesajlardan birini bilmesi halinde diğer mesajı da bulabileceği ortadadır. Daha da kötüsü mesajların genel olarak yapıları belirlidir, örneğin ilk 20 sekizli IP başlığını ifade eder gibi. Bu veriler ve sözlük saldırıları (Dictionary Attack) da kullanılarak açık mesajlardan herhangi biri bilinmeden her iki mesaj da çözülebilir. Saldırganın ağı dinlemeye devam etmesi ile aynı IV dolayısıyla aynı anahtar dizisini kullanan bir başka paket daha yakalaması mümkündür. Bu şekilde aynı IV değerini kullanan mesajlar arttıkça mesajların çözülmesi daha kolay hale gelir [8, 9, 11]. Bu saldırıda saldırgan gizli anahtarı ele geçirmese de mesajları çözerek okuyabilir duruma gelmiştir. Saldırgan haberleşmeyi izlemeyi sürdürerek belirli miktarda veri elde ettiğinde mesajların şifreli ve açık hallerini de kullanarak doğrudan anahtarı elde etmeye de yönelebilir, fakat anahtarın elde edilmesi için daha kolay metotlar da mevcuttur.

IEEE 802.11-1999 standardında tanımlanan IV' nin boyu 24 bit yani üç sekizlidir. Her şifreleme işleminde kullanılan IV değeri, paketi alacak tarafın şifreyi çözebilmesi için paketin içine açık bir biçimde yazılır. IV' nin bilinmesi gizli anahtarın bilinmediği durumda hiç bir anlam ifade etmez. Burada dikkat edilmesi gereken durum ise aynı IV değerinin aynı anahtar için birden fazla kere kullanılmamasıdır. IV alanının 24 bit olması 2^{24} = 16.777.216 farklı IV değerinin olabileceğini gösterir. Oldukça yüksek görünse de ortalama yoğunluktaki 11 Mbps kapasiteli erişim noktasının saniyede 700 paket gönderdiği düşünüldüğünde IV alanı 7 saat içerisinde tüketilecektir. IV alanı tüketildikten sonra anahtar değişimi yapılmaması durumunda aynı anahtar ve IV ile şifrelenecek paketler gönderilmeye başlanacak, bu durumda sürekli hattı dinleyecek saldırgan yapacağı analizler sonucunda mesajları çözebilecek ve gizli anahtarı elde edebilecektir.

Aynı IV değerinin kullanılmaya başlanması için 7 saat geçmesi de gerekmeyebilir. Bir çok gerçeklemede cihazlar ilk açıldıklarında IV değeri sıfırdan başlatılarak birer artırılarak seçilir. Bu durumda haberleşmeye katılan her yeni cihaz başta aynı anahtar ve IV değeri ile şifrelemeye başlayacaktır. Aynı anahtar ve IV ile şifrelenmiş birden fazla veri paketi olmuş olacaktır.

IV değerinin rasgele seçilmesi IV yeniden kullanımını engelleyemeyecektir. Doğum-günü paradoksu adı verilen olasılık hesabına göre IV değerleri rasgele seçilse de ortalama 5000 paket içerisinde [9] aynı IV değerini kullanmış birden fazla şifreli paket bulmak mümkündür.

3.4.5.2 RC4 Zayıf Anahtarları

Şifreleme işleminde kullanılan RC4 algoritması temelde rasgele sayı üretilmesine dayanır. Açık veri üretilen rasgele sayılar ile dışlamalı veya işlemine tabi tutularak şifrelenmiş olur. Algoritma bu özelliği ile en güvenilir şifreleme mekanizmalarından biri olarak kabul edilen Vernam algoritmasıyla benzerlikler taşımaktadır. Vernam algoritmasının güvenilir olması kullanılan anahtar dizisinin gerçek rasgele sayılar olmasına dayanır. Gerçekte de RC4 algoritması gerçek rasgeleye yakınlıkta değerler üretebilir. Rasgele sayı dizisinin RC4 ile mi üretildiği yoksa gerçek rasgele sayılar mı olduğunu anlamak için ortalama 1 G-sekizlilik verinin incelenmesi gerekir [12].

Fluhrer ve diğ. [13] 2001 yılında yaptıkları çalışmada RC4 rasgele sayı dizisinin (anahtar dizisi) oluşturulmasında özellikle bazı ilklendirme değerleri [IV||Anahtar] için oluşturulan ilk sekizlilerin rasgele sayılar olmadığını, oluşturulan ilk rasgele sekizlilerin belirlenmesinde ilklendirme değerinin bazı bitlerinin hiç bir anlam ifade etmediğini ortaya koymuşlardır. Daha da kötüsü bu sözde rasgele sayılar kullanılarak açık verinin genellikle yapıları kolayca tahmin edilen başlık alanları şifrelenmektedir ve açık verinin bilinmesiyle anahtar dizisine ve oradan da anahtara saldırı düzenlenebilir.

RC4 algoritmasının üreticisi konumundaki RSA güvenlik firmasının bu konuda yaptığı açıklamada RC4-PRNG' den üretilecek ilk 256 sekizlinin kullanılmaması gerektiği belirtilmiştir. Fakat bu çözüm hali hazırda kullanılan cihazlara yansıtılamayacağından göz ardı edilmiştir.

3.4.5.3 Doğrudan Gizli Anahtara Yönelik Saldırılar

Zayıf anahtarlarla üretilen anahtar dizisinin ilk sekizlilerinin rasgele olmaması ve bu sekizlilerle içeri çoğunlukla tahmin edilebilen başlık alanlarının şifrelenecek olması kullanılarak gizli anahtarın tamamı ele geçirilebilir [13, 14]. Ayrıca içeri bilinen mesajların şifrelenmesi ve şifreli hallerinin yakalanarak analiz edilmesiyle de gizli anahtara ulaşılabilir [11].

Anahtar boyunun 40 bitten, 104 bite çıkartılması anahtarın çözülmesi zamanını 2,5 katına çıkarır, yani anahtar boyu ile çözülmesi arasında lineer bir bağlantı mevcuttur [8].

4 802.11i-2004 STANDARDI VE GETİRDİKLERİ

802.11i-2004 standardı 802.11x ağları için yeni güvenlik standardıdır. 802.11-1999 standardındaki güvenlik açıklarının zaman içerisinde ortaya çıkması ve bu açıklıkların temel mantık hatalarından kaynaklanması, hataların yamanamaz olması ve yeni bir güvenlik protokolü oluşturulması sonucunu doğurmuştur. Yapılan çalışmalarda ele alınan başlıca konular şunlardır:

- Karşılıklı kimlik doğrulama
- Anahtar hiyerarşisi ve dağıtımı
- Şifreleme metotları

IEEE 802.11i karşılıklı asıllama ve anahtar yönetimi için 802.1X standardını [15] kullanır. Genel dört anahtar yerine her istemci için farklı olacak, tekli-aktarım mesajlarında (unicast) kullanılacak bir anahtar (karşılıklı haberleşme anahtarı) ve her istemci için aynı olacak, çoklu aktarımda kullanılacak başka bir anahtar (grup anahtarı) tanımlar. Mesajların şifrelenmesinde kullanılmak üzere WEP yerine yine WEP gibi RC4 şifreleme algoritmasını kullanan TKIP (Temporal Key Integrity Protocol) ve AES (Advanced Encryption Standart) şifreleme algoritmasını kullanan CCMP (Counter Mode/ CBC-MAC Protocol) isimli iki farklı mekanizma tanımlar.

4.1 Kimlik Doğrulama

802.11i karşılıklı kimlik doğrulama ve anahtar yönetimi için 802.1X standardını kullanır. 802.1X, IEEE 802.x yerel alan ağları için tasarlanmış port temelli ağ erişim denetimi mekanizmasıdır. Temel olarak telli ağlar (802.3/Ethernet ağları) için tasarlanmış olsa da telsiz ağ uygulamasında da kullanılmaktadır.

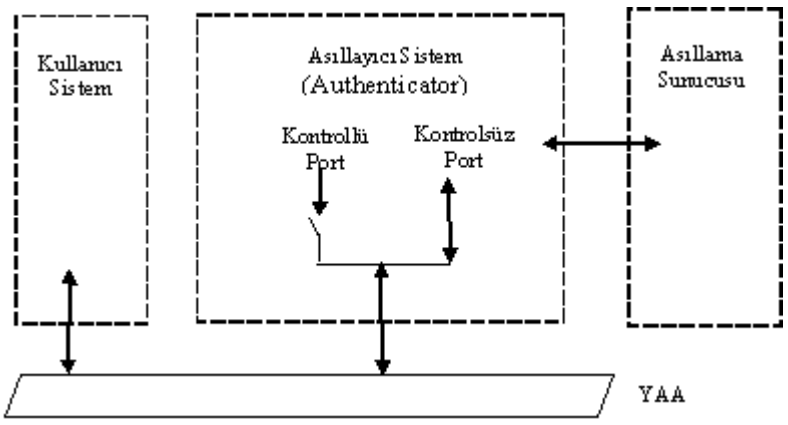
802.x ağların ortak özellikleri yetkilendirilmemiş cihazların fiziksel olarak ağa bağlanabilme olasılığının yüksek olması yada ağa bağlanmış cihazlar üzerinden yetkilendirilmemiş kullanıcıların ağa erişim imkanlarının bulunmasıdır. Örneğin misafir kabul salonunda ağa bağlantı portu bulunan bir işyerine ait yerel alan ağı gösterilebilir. Böyle bir durumda kullanıcı denetimi yapılmaksızın her türlü ağ

servisine erişim imkanı sunulması arzu edilmeyen bilgi sızıntılarına neden olabilir. Telli ortamlar için fiziksel güvenlik daha kolay sağlanırken telsiz ortamlar için fiziksel yalıtımın sağlanması daha zordur. Bu nedenle telsiz ağlarda erişim mekanizmasının uygulanması daha gerekli bir hal almaktadır.

4.1.1 802.1X

Yerel alan ağlarına bağlanan, erişen cihazlara sistem; bu sistemlerin yerel alan ağlarına bağlanma noktalarına port adını verelim. Sistemlere ait bu portlar, sistemlerin yerel alan ağına bağlı diğer sistemlerin sağladığı ağ servislerine erişimini sağlarlar. Aynı zamanda sistem tarafından yerel alan ağındaki diğer sistemlerin kullanımına açılacak servisler içinde bir erişim noktası oluştururlar. IEEE 802.1X erişim denetimi mekanizması sistemlere ait bu portların yalnız ve yalnız yetkilendirilmiş cihaz ve kullanıcılar tarafından açılması ve kullanılmasına imkan verir. Port erişim mekanizmasında tanımlı üç farklı öğe mevcuttur ve Şekil 4-1'de gösterilmişlerdir:

- Asıllayıcı (authenticator): Sağladığı ağ servislerine erişim için diğer ağ unsurlarına asıllama sorgusunda bulunan öğe.
- Kullanıcı (supplicant): Asıllayıcının sağlayacağı hizmetlerden faydalanmak isteyen, kimliğini ispatlaması gereken öğe.
- Asıllama Sunucusu (Authentication Server): Kullanıcı tarafından sunulan kimlik bilgilerinin doğrulunu kontrol eden, kullanıcının ağ servislerine erişim yetkisi olup olmadığı kararını verecek olan öğe.

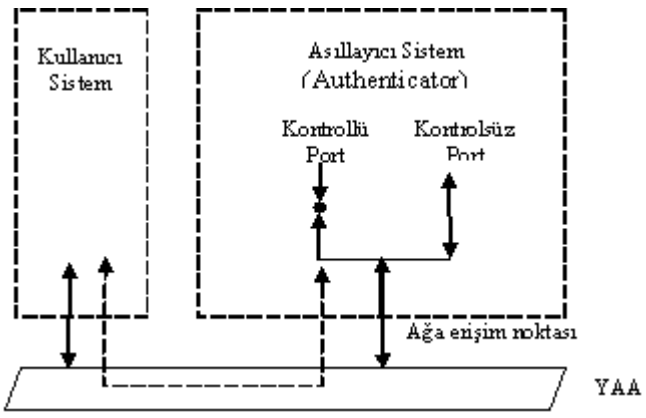


Şekil 4-1: Port Erişim Mekanizması

Asıllıyıcı sistem üzerindeki kontrolsüz port asıllayıcı sistem ile ağa bağlı diğer sistemler arasında herhangi bir kontrol olmaksızın veri alış verişinde kullanılır. Kontrollü port ise yalnız ve yalnız kullanıcı kimliğinin tanınmasından sonra veri iletişiminde kullanılır. Kontrolsüz port kimlik doğrulama işlemi için kullanılacak portokole ait bilgilerin taşınmasında kullanılırken, kontrollü port asıllayıcı sistem tarafından sunulan hizmetlerin verildiği nokta olarak düşünülebilir. Mevcut sistemde ayrı bir asıllama sunucusu bulunabileceği gibi asıllama sunucusu asıllayıcı üzerinde de gerçekleştirilmiş olabilir.

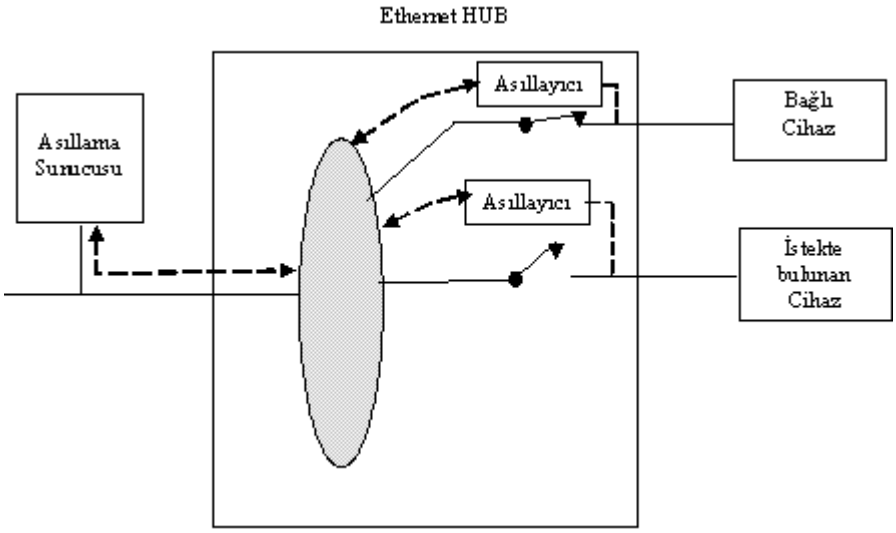
Asıllama işlemi için EAP (Extensible Authentication Protocol) protokolü kullanılır [16, 17]. Temelde PPP (Point-to-Point) protokolü için tasarlanan EAP protokolü verilerinin yerel alan ağı üzerinden taşınmasında da EAPOL (EAP over LANs) protokolü kullanılmaktadır. Asıllayıcı ile asıllama sunucusu arasında yapılacak haberleşmenin ne şekilde yapılacağı 802.1X standardında belirtilmemiş olsada tipik olarak EAP protokolü bilgilerinin daha üst seviye bir protokol tarafından taşınmasıyla, örneğin RADIUS (Remote Authentication Dial-In User Service) tarafından taşınacak EAP paketleri ile bu haberleşme gerçekleştirilebilir.

Kullanıcı ile asıllayıcı sistemlerin ilk karşılaşmalarından sonra asıllayıcı sistem kullanıcıdan kimliğini ispatlamasını isteyebileceği gibi kullanıcı kimlik ispatlama mekanizmasını kendi de başlatabilir. Koşturulacak kimlik doğrulama mekanizmasından sonra kullanıcı için olumlu yada olumsuz bir sonuç oluşabilir. Asıllamanın başarısız olması durumunda kullanıcı asıllayıcı tarafından verilen ağ hizmetlerinden yararlanamaz. Başarılı olması durumunda ise asıllayıcının Kontrollü Port' u kullanıcıya hizmet sunmaya başlar. Şekil 4-2 kontrollü port erişimini göstermektedir:



Şekil 4-2: Kontrollü-port erişimi

Ağa erişim noktası fiziksel bir port olabileceği gibi kullanıcıya birebir etkileşim olanağı sunan mantıksal bir port da olabilir. Fiziksel port örneği olarak Ethernet ağlarında kullanılan HUB ve HUB' a ait tüm bağlantı portları gösterilebilir. Hali hazırda bulunan Anahtar cihazlarının ve HUB cihazlarının bazılarında 802.1X özelliği mevcuttur. Şekil 4-3, 802.1X protokolünün HUB tarafından kullanımını göstermektedir.



Şekil 4-3: 802.1X protokolü kullanımı örneği

Telsiz ağlarda yukarıdaki şekildeki gibi fiziksel bağlantı yoktur. Onun yerine her bir telsiz ağ istemcisi ile erişim noktası arasında kurulan mantıksal bağlantıdan söz edilir (association). Benzer şekilde telsiz ağ istemcisinin erişim noktasının sunduğu ağ hizmetlerinden faydalanabilmesi için öncelikle asıllama işleminin gerçekleşmesi gereklidir.

4.1.2 802.11 ve 802.1X

IEEE 802.11, dağıtım omurgası ile yetkilendirilmemiş kullanıcılar arasındaki veri alış-verişi akışında yukarıda özetlenen kontrollü port/ kontrolsüz port lojiğine dayanan 802.1X' i kullanır. 802.1X asıllayıcısı ile kullanıcılar arasındaki kimlik doğrulama haberleşmesini tanımlayan EAP paketleri 802.11-veri paketleri olarak 802.11 çerçeveleri içerisinde taşınır. Kimlik asıllama mekanizmasına ait EAP paketleri kontrolsüz port üzerinden, kimlik asıllama mekanizmasına ait olmayan veri paketleri de kontrollü port üzerinden alınır ve gönderilir. 802.11 ağlarında 802.1X asıllayıcısı erişim noktası, 802.1X kullanıcısı telsiz ağ adaptörü bulunan herhangi bir

kullanıcı olarak düşünülebilir. Böylece kimliğini henüz ispatlamamış kullanıcılara ait veri paketleri erişim noktası tarafından işlenmez. İki kullanıcı arasındaki her bir iletişim birliği (association) ayrı bir 802.1X portu tanımlar ve kimlik asıllama bu port için gerçekleştirilir.

802.11 veri trafiğinin korunmasında kullanacağı kriptolojik anahtarların oluşturulmasında ve güncellenmesinde 802.1X ve EAPOL-Anahtar dört yollu el sıkışma ve iki yollu grup anahtarı el sıkışması mekanizmalarının tanımlar ve kullanır. Anahtarlar, kimlik asıllama işleminin tamamlanmasından sonra oluşturulur ve belli sayıda verinin gönderilmesi, zamanlayıcılar gibi nedenlerden dolayı güncellenebilir. Dört yollu el sıkışma ve iki yollu grup anahtarı dağıtımı mekanizmaları ileriki bölümlerde ele alınacaktır

4.1.3 EAP

EAP (Extensible Authentication Protocol [16, 17]) IETF tarafından PPP haberleşmesinde karşılıklı kimlik doğrulama amacıyla geliştirilmiş bir protokoldür. EAP' nin kendisi herhangi bir kimlik doğrulama mekanizması tanımlamaz. Bunun yerine kullanılacak herhangi bir kimlik doğrulama mekanizması için bir altyapı oluşturur. EAP karşılıklı kimlik doğrulama işleminde kullanılmak üzere mesajlar kümesi tanımlar. Bu mesajlar daha üst seviye kimlik doğrulama mekanizmaları tarafından kullanılır. EAP ayrıca karşılıklı kimlik doğrulama işleminde bulunacak öğeler için tip spesifik kimlik doğrulama bilgilerinin taşınacağı bir alt yapı oluşturur. EAP' nin genişletilebilir olmasını sağlayan özellik bu herhangi bir kimlik doğrulama mekanizması tanımlamaması ve ileride oluşturulacak kimlik doğrulama algoritmalarının bilgilerinin taşınması için bir alt yapı oluşturmasından ileri gelir. EAP tarafından taşınacak kimlik doğrulama metotlarının tanımlanması RFC' ler yolu ile yapılır. Örneğin RFC-2246 TLS (Transport Layer Security) protokolünün EAP kullanılarak nasıl kullanılacağını tanımlar [18].

EAP protokolünün tanımlandığı [16] dört tip EAP mesajı tanımlar:

- İstek (Request): Asıllama işlemini yapacak öğe tarafından istemciye gönderilen mesajları tanımlar
- Yanıt (Response): İstemci tarafından asıllayıcıya gönderilecek mesajları tanımlar.

- Başarılı (Success): Asıllayıcı tarafından gönderilen ve kimlik doğrulama işleminin başarılı olduğunu belirten mesajları tanımlar.
- Başarısız (Failure): Asıllayıcı tarafından gönderilen ve kimlik doğrulama işleminin başarısız olduğunu belirten mesajları tanımlar.

4.1.3.1 EAP Paket Formatı

RFC-3748' de tanımlanan EAP mesaj formatı Şekil 4-4'de verilmiştir:

Şekil 4-4: EAP paketi formatı

Kod: 1 sekizli uzunluktaki bu alan mesajın tipini tanımlar:

- (01): İstek
- (02): Yanıt
- (03): Başarılı
- (04): Başarısız

Kimlik: 1 sekizli uzunluğundaki bu alan gönderilen ve alınan mesajların sıra numaraları gibi düşünülebilir. Yanıt olarak gönderilecek mesajlar, yanıtı olduğu isteğin taşıdığı kimlik bilgisini aynen taşırlar. Bunun dışında gönderilen her mesajda bir arttırılır.

Uzunluk: 2 sekizli uzunluğundaki bu alan EAP paketinin toplam uzunluğunu gösteren bilgidir. EAP başlığını da (kod alanından başlayarak) kapsar.

Veri: Değişken uzunluklu, kimlik doğrulama bilgilerini taşır. Veri alanındaki bilginin yorumlanması Kod alanı değerine göre yapılır.

Başarılı veya başarısız mesajları asıllayıcı tarafından istemciye gönderilen EAP spesifik kimlik doğrulama işleminin sonucunu bildiren mesajlardır. Herhangi bir bilgi içermeyen 4 sekizlilik paketlerdir, yalnızca kimlik doğrulama işleminin başarılı olup olmadığını istemciye bildirirler.

4.1.3.2 EAP İstek ve Yanıt Paketleri

EAP istek ve yanıt paket formatı aşağıda verilmiştir. Kod alanı istek (0x01) veya yanıt (0x02) olabilir. EAP İstek ve Yanıt paketleri yapısı Şekil 4-5'de verilmiştir.

Şekil 4-5: EAP-İstek ve EAP-Yanıt paketleri yapısı

Tip: 1 sekizli uzunluğundaki bu alan isteğin veya yanıtın ne tür bir istek veya yanıt olduğunu belirler. RFC-3748 tarafından tanımlanan tipler şunlardır:

- 1 Identity
- 2 Notification
- 3 Nak (Response only)
- 4 MD5-Challenge
- 5 One Time Password (OTP)
- 6 Generic Token Card (GTC)
- 254 Expanded Types
- 255 Experimental use

Yukarıda sıralanan EAP istek/yanıt tiplerinden ilk dördünün gerçekleştirilmesi zorunludur ve ne şekilde gerçekleneceği RFC-3748' de anlatılmıştır. Bunların dışında kalan tip tanımlamaları yine RFC' ler ile tanımlanacaktır ve bu tiplere ait tip kodunun ne olacağı IANA (Internet Assigned Numbers Authority) tarafından belirlenecektir.

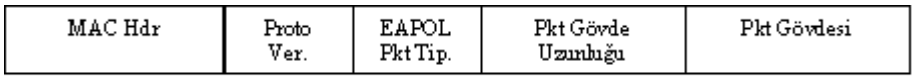
4.1.4 EAPOL

EAP protokolü modem kullanılarak oluşturulan çevirmeli ağlar için kimlik doğrulama amacıyla tasarlanmış olduğundan 802.x ağları için ne şekilde taşınacağı belirtilmemiştir. Bu nedenden dolayı EAP protokolünü karşılıklı kimlik doğrulama amacıyla kullanan 802.1X protokolünde EAP paketlerinin 802.x ağlarında ne şekilde

taşınacağını belirleyen EAPOL (EAP Over LAN's) protokolü tanımlanmıştır. Tanımlanan bu protokol sayesinde EAP paketleri asıllayıcı ile istemci arasında 802.x ağları üzerinden taşınabilecektir. 802.1X standardı EAPOL protokolünün açıklamasını yapar ve IEEE 802.3 ve Token Ring ağları için paket yapılarının ne şekilde olması gerektiğini açıklar.

4.1.4.1 EAPOL Paket Formatı

802.1X standardında EAPOL paketleri için tanımlanmış paket formatı Şekil 4-6'da verilmiştir:



Şekil 4-6: EAPOL paketi yapısı

802.1X standardı tarafından EAPOL protokolüne atanmış Ethernet paket tipi numarası (0x88-8e)' dir.

Versiyon: 802.1X standardı tarafından tanımlanan EAPOL versiyon numarası (0x01)' dir.

Paket Tipi: 802.1X' te tanımlanan EAPOL paket tipleri şunlardır:

- EAPOL-Başlat (0x01)
- EAPOL-Anahtar (0x03)
- EAP-Paket (0x00)
- EAPOL-Logoff (0x02)
- EAPOL-Alarm (0x04)

Paket tipinin EAP-Paket, EAPOL-Anahtar veya EAPOL-Alarm olması durumunda pakete ait bir gövdenin varlığından söz edilir ve paket gövde uzunluğu sıfırdan farklıdır. Diğer paket tipleri için paket gövde uzunluğu sıfırdır ve paket gövdesi yoktur.

EAPOL-Logoff mesajı istemcinin ağdan ayrılmak istediğini asıllayıcıya bildirir.

EAPOL protokolünün oluşturulma amacı olan EAP paketlerinin 802.x ağları üzerinden taşınması için kullanılan paket tipi EAP-Paket' tir. Bu durumda EAPOL paketleri, EAP paketleri için yalnızca bir konteynır vazifesi görürler.

EAPOL-Alarm mesajı WPA/RSN tarafından kullanılmaz.

4.1.4.2 EAPOL-Başlat

EAPOL-Başlat mesajı istemciler tarafından, IEEE 802.1X asıllayıcıları için ayrılmış özel yayın adresine (01-80-C2-00-00-03) gönderilir. Bu mesaj sayesinde istemci ortamda bulunması muhtemel asıllayıcıları bulabilir ve asıllayıcılara kimliğini ispatlamak isteyen bir istemcinin var olduğunu bildirmiş olur.

Bir çok durumda asıllayıcı yeni bir istemcinin bağlanmak istediğini donanımsal sinyaller ile anlayabilir. (Örneğin Ethernet HUB' ın bir portuna bağlanan kablonun varlığından veya 802.11 ağlarında olduğu gibi öncelikle haberleşme birliği (association) oluşturulmasından) Böyle bir durumda asıllayıcı istemcinin EAPOL-Başlat mesajını beklemeden paket tipi EAP-Paket olan EAPOL çerçevesine yerleştirilmiş EAP-İstek-kimlik mesajını istemciye gönderebilir.

4.1.4.3 EAPOL-Anahtar

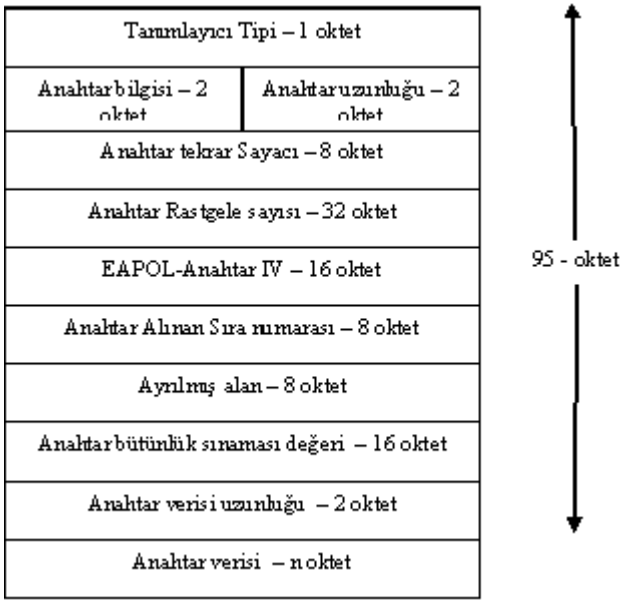
EAPOL-Anahtar paketleri, kimlik doğrulama işlemi başarıyla sonuçlanması durumunda istemciye geçerli anahtarların aktarılması amacıyla kullanılır. Taşınacak anahtarların bir başka anahtarla şifrelenmesi ve bütünlük sınamasının yapılması gereklidir. 802.1X bu anahtar koruma işleminin nasıl yapılması gerektiğini tanımlamamıştır. 802.1X EAPOL-Anahtar paketlerinin yapısını tanımlamış olsa da 802.11i standardı bu yapıyı kullanmaz, onun yerine kendi EAPOL-Anahtar paket yapısını tanımlar.

802.11 istemci ile asıllayıcı arasında kriptolojik anahtarların oluşturması ve güvenlik birliklerinin karşılıklı senkronize edilmesiyle sonuçlanan EAPOL-Anahtar paket akışını tanımlar. 802.11 tarafından tanımlanan ve EAPOL-Anahtar paketlerinin kullanıldığı 3 farklı anahtar değiş-tokuşu mevcuttur:

- 4-yollu el sıkışma, karşılıklı şifreleme amaçlı anahtarların oluşturulmasında ve grup anahtarının istemciye aktarılmasında kullanılır.
- Grup anahtarı el sıkışması, yenilenen grup anahtarının istemcilere aktarılmasında kullanılır.

- İstemci-istemci arası anahtarın oluşturulmasında kullanılır.

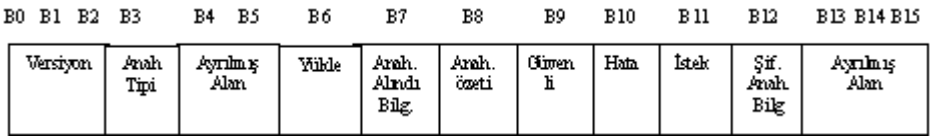
802.11i tarafından oluşturulmuş EAPOL-Anahtar paketi yapısı ve alt alanlarının taşıdıkları anlamlar Şekil 4-7'de verilmiştir:



Şekil 4-7: EAPOL-Anahtar paketi yapısı

Tanımlayıcı Tipi: EAPOL-Anahtar paketinin ne tip bir anahtar bilgisi içeriyor olduğunu ve diğer alt alanların ne şekilde yorumlanması gerektiğini bildiren 1 sekizlilik bir alandır. 802.1X [15] standardında bu alan için belirlenmiş tek değer (0x01) ile RC4 Anahtar tanımlayıcı tipidir. Bu tez yazıldığı sıralarda IEEE, 802.1X protokolünün düzeltilmiş yeni standardını çıkarmak üzereydi ve bu alan için en azından AES Anahtar tanımlayıcı tipinin de eklenmiş olması kuvvetle muhtemeldir.

Anahtar bilgisi: Taşınan anahtar ile ilgili ayrıntılı bilgilerin kodlandığı 2 sekizlilik bir alandır. Anahtar bilgisi alt alanları 802.11i standardında tanımlanmış ve Şekil 4-8 ile verilmiştir:



Şekil 4-8: EAPOL-Anahtar paketi Anahtar bilgisi alt alanları

-- Versiyon: Anahtar bilgisi alanı kodlama versiyon numarasını gösteren 3 bitlik alandır. (001) ve (010) değerleri tanımlanmıştır:

- (001): Karşılıklı şifreleme veya grup şifreleme işlemlerinin hiçbirinde CCMP algoritması kullanılmayacaksa, bu alana (001) değeri yazılır. Bu değerin ifade ettiği anlam:
    - EAPOL-Anahtar bütünlük koruması için HMAC-MD5 [19, 20] algoritmasının kullanılacağını bildirir.
    - EAPOL-Anahtar, anahtar verisinin şifrelenmesinde RC4 algoritmasının kullanılacağını bildirir.
- (010): Karşılıklı şifreleme veya grup şifreleme işlemlerinin herhangi birinde CCMP algoritması kullanılacaksa, bu alana (010) değeri yazılır. Bu değerin ifade ettiği anlam:
    - EAPOL-Anahtar bütünlük koruması için HMAC-SHA1-128 [19, 21] algoritmasının kullanılacağını bildirir. SHA1 özetinin en anlamlı ilk 128 biti özet değeri olarak kullanılır.
    - EAPOL-Anahtar, anahtar verisinin şifrelenmesinde NIST AES anahtar sarmallama algoritmasının [22] kullanılacağını bildirir.

-- Anahtar Tipi: 1 bitlik (B3) bu alan EAPOL-Anahtar paketinin karşılıklı şifrelemede kullanılacak geçici anahtarın (PTK) oluşturulması amacıyla kullanılıp kullanılmadığını gösterir. PTK oluşturulması için yürütülen 4-yollu el sıkışma paketleri için bu alan kurulurken, aksi durumlar (GTK ve STA-Anahtarı) için kurulmaz.

-- Ayrılmış Alanlar: B3,B4, B13-B15 bitleri ileriki kullanımlar için ayrılmıştır. Gönderici bu alana sıfır değerini yazar. Alıcı tarafta bu alanda yazan veri işlenmez.

-- Yükle: Bir bitlik (B6) bu alan Anahtar Tipi alanı ile birlikte yorumlanır.

- Anahtar Tipi (B3) alanında sıfır yazması durumunda bu alana gönderici tarafından sıfır yazılmalı ve alıcı tarafta da herhangi bir işleme tabi tutulmamalıdır.
- Anahtar Tipi (B3) alanında bir yazması durumunda:

- Yükle (B6) alanında sıfır yazması durumunda oluşturulan karşılıklı veri şifreleme işleminde kullanılacak geçici anahtarın veri şifreleme için kullanıma hazır olmadığını belirtir.
- Yükle (B6) alanında bir yazması durumunda oluşturulan karşılıklı veri şifreleme işleminde kullanılacak geçici anahtarın hazır olduğu ve veri şifreleme işlemi için üretilmiş geçici anahtarın kullanılması gerektiğini belirtir.

-- Anahtar Alındı Bilgisi: Bir bitlik (B7) bu alan asıllayıcı tarafından alındı bilgisi istenilen EAPOL-Anahtar paketlerinde kurulur. Bu biti kurulmuş bir EAPOL-Anahtar paketi alan istemci oluşturacağı yanıt paketinde sıra numarası değerine kendisine gelen EAPOL-Anahtar paketindeki sıra numarası değerini aynen kopyalar.

-- Anahtar Özeti: Bir bitlik (B8) bu alan EAPOL-Anahtar paketinde yer alan Anahtar bütünlük sınaması alanında geçerli bir değer olup olmadığını ve bütünlük sınaması yapılması gerekip gerekmediğini ifade eder.

-- Güvenli: Bir bitlik (B9) bu alan başlangıçtaki anahtar değişiminin tamamlanmasından sonra kurulur, istemcinin durum makinesini kontrol amaçlı kullanılır. Asıllayıcı göndereceği tüm EAPOL-Anahtar paketlerinde eğer istemci karşılıklı şifrelemede kullanılacak geçici anahtara (PTK) ve grup şifreleme anahtarına (GTK) sahip değilse sıfır yazar. İstemcinin bu anahtarlara sahip olması durumunda ise asıllayıcı göndereceği EAPOL-Anahtar paketlerinin bu bitini kurar. İstemci PTK ve GTK anahtarlarına sahip olmadan ve asıllayıcıdan bu biti kurulmuş herhangi bir paket almadan bu biti kurmaz. Diğer durumda istemci göndereceği tüm EAPOL-Anahtar paketlerinde bu biti kurar.

-- Hata: Bir bitlik (B10) bu alan istemci tarafından asıllayıcıya TKIP protokolü ile korunmuş paketlerde mesaj bütünlüğü değeri hatalı bir mesaj alındığını bildirmek amacıyla kurulur. Bu biti kurarak mesaj bütünlüğü hatasını asıllayıcıya bildirecek olan istemci aynı zamanda İstek bitini (B11) de kurmalıdır.

-- İstek: Bir bitlik (B11) bu alan istemcinin, bütünlük değeri hatalı bir paket aldığını asıllayıcıya bildirmesi için veya istemcinin 4-yolu el sıkışmanın asıllayıcı tarafından başlatılmasını istediğini asıllayıcıya bildirmesi için kullanılır. Hali hazırda yürütülen 4-yollu el sıkışma işlemlerinde bu bit istemci tarafından kurulmaz.

Asıllayıcı bu biti hiç bir durumda kurmaz. Anahtar Alındı Bilgisi biti kurulu hiç bir paket için bu alan kurulamaz. Michael bütünlük değeri hatası paketleri (hata ve istek bitleri kurulu paketler) yeni 4-yollu el sıkışma isteği demek değildir, fakat asıllayıcı isterse bu tip bir paket aldığında yeni bir 4-yollu el sıkışma mekanizması başlatabilir. Asıllayıcı İstek (B11) ve Anahtar Tipi (B3) kurulu bir paket aldığında yeni bir 4-yollu el sıkışma işlemi başlatır. Anahtar Tipi (B3) kurulu olmayan istek paketleri için asıllayıcı grup anahtarını (GTK) değiştirir, isteği gönderen istemci ile yeni bir 4-yollu el sıkışma işlemi başlatır ve bu işlemden sonra kendisine bağlı tüm diğer istemcilerle Grup anahtarı değişimi (2-yollu el sıkışma) işlemini yürütür.

-- Şifreli Anahtar Bilgisi: Bir bitlik (B12) bu alan EAPOL-Anahtar paketinde yer alan anahtar verisinin şifrelenip şifrelenmediğini belirten bayraktır.

Anahtar Uzunluğu: Karşılıklı şifreleme işleminde kullanılacak algoritmanın anahtar uzunluğunu sekizli cinsinden ifade eder. 802.11i' de tanımlı anahtar uzunlukları Tablo 4-1'de verilmiştir:

Tablo 4-1: Şifreleme algoritmaları anahtar boyları

Şifreleme Algoritması	CCMP	TKIP	WEP-40	WEP-104
Anahtar Uzunluğu (sekizli)	16	32	5	13

Anahtar Tekrar Sayacı: Protokolün tekrar paketlerini anlaması için kullanılan 8 sekizlik bir sayaçtır. Karşılıklı Asıl Anahtar (PMK-Pairwise Master Key) oluşturulduğunda sıfır ilk değeri verilir. Sayacın artırılması asıllayıcı tarafından yapılır. İstemci asıllayıcının bir mesajına yanıt vereceği zaman almış olduğu son geçerli EAPOL-Anahtar paketinde yer alan sayaç değerini aynen kopyalar. Karşılıklı şifrelemede kullanılacak geçici anahtarın (PTK) oluşturulmasında tekrar sayacının performans eniyileme işlemi dışında herhangi bir işlevi yoktur, fakat grup anahtarı değişimi işlemi sırasında anlamlı bir rol üstlenir.

Anahtar Rasgele Sayısı: 32 sekizlilik bu alan EAPOL-Anahtar paketlerinde asıllayıcı ve istemcilerin ürettikleri ve anahtar türetilmesinde de kullanılan "Snonce" ve "Anonce" değerlerini taşır.

EAPOL-Anahtar IV: EAPOL-Anahtar paketlerinde taşına şifrelenmiş anahtarların şifrelenmesi sırasında kullanılan ilklendirme vektörünü taşıyan 16 sekizlilik bir

alandır. Anahtar Şifreleme Anahtarı (KEK-Key Encryption Key) ile birlikte kullanılır.

Anahtar Alınan Sıra Numarası: 8 sekizli uzunluğundadır. 4-yollu el sıkışma mekanizmasının 3. adımında ve grup anahtarı değişimi mekanizmasının ilk adımında 802.11 cevaplarının senkronize edilmesinde kullanılır. Ayrıca Michael mesaj bütünlüğü hatası mesajlarında hangi pakete ilişkin hata olduğunu belirtmek üzere hatalı mesaja ait paket sıra numarası değerini de taşır.

Anahtar Bütünlük Sınaması Değeri: EAPOL-Anahtar paketinin başlangıcından anahtar verisinin sonuna kadar olan bütünlük sınaması değerinin taşındığı alandır ve 16 sekizli ile ifade edilir. Bütünlük sınaması hesabı sırasında bu alan sıfırlanır. Anahtar verisi şifrelenecekse, şifreleme işlemi bütünlük hesabından önce yapılır. Bu alanın hesabında tanımlayıcı tipinin bir olması durumunda HMAC-MD5 [19, 20], tanımlayıcı tipinin iki olması durumunda HMAC-SHA1-128 [19, 21] algoritmaları kullanılır.

Anahtar Verisi Uzunluğu: EAPOL-Anahtar paketinde taşınan anahtar verisinin uzunluğunu ifade eden 2 sekizlilik alandır. Şifreleme işlemi yapıldı ise şifreleme işleminden sonraki uzunluğu gösterir, herhangi bir dolgulama yapıldıysa dolgu uzunluğunu da kapsar.

Anahtar Verisi: Anahtar türetilmesi aşamalarında ihtiyaç duyulan ve EAPOL-Anahtar paketinin sabit alanlarında içerilmeyen değişken uzunluklu bilgilerin taşındığı alandır. Bu alanda taşınacak bilgiler bilgi elemanları (IE-Information Elements-örneğin RSN IE) olabileceği gibi doğrudan anahtar verisi (örneğin grup anahtarı) da taşınabilir. Bu alanda taşınacak veriler için hazırlanmış bir veri taşıma formatı mevcuttur ve Şekil 4-9 ile verilmiştir:

Tip	Uzunluk	OUI	Veri tipi	Veri
1 oktet	1 oktet	3 oktet	1 oktet	(uzunluk -4) oktet

Şekil 4-9: Anahtar verisi alt alanı formatı

-- Tip: Taşınan verinin ne tip bir veri olduğunu ifade eder. RSN IE için (0x30) kullanılırken anahtar verisin bu alana (0xdd) değeri yazılır.

-- Uzunluk: OUI' dan başlayacak şekilde taşınan verinin uzunluğunu sekizli cinsinden ifade eden 1 sekizlilik bir alandır.

-- OUI: Taşınan anahtar verisinin ne tip bir anahtara ait olduğunu veri tipi alanı ile birlikte belirler. Tanımlı değerler Tablo 4-2'de verilmiştir:

Tablo 4-2: OUI Alt alanı olası değerleri

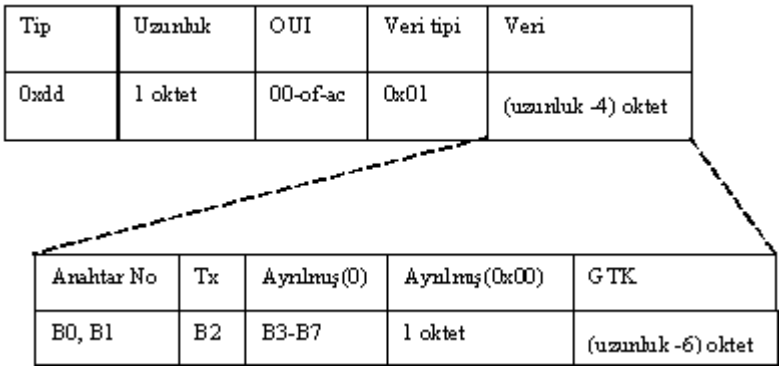
OUI	Veri Tipi	Anlamı
00-0F-AC	0	Ayrılmış değer
00-0F-AC	1	Grup anahtarı verisi
00-0F-AC	2	STA anahtarı verisi
00-0F-AC	3	MAC Adresi anahtarı verisi
00-0F-AC	4	PMKID anahtarı verisi
00-0F-AC	5-255	Ayrılmış değer
Üretici OUI	0-255	Üretici spesifik
Diğer	0-255	Ayrılmış değer

EAPOL-Anahtar paketinde yer alacak bilgi elemanlarını veya anahtar bilgilerini yorumlayamayan istemci ve/veya asıllayıcılar bu paketleri geçersiz kılarak işlemezler.

Anahtar verisi alanı şifrelenecekse ve şifreleme algoritması olarak AES anahtar sarmallama algoritması [22] kullanılacaksa ve eğer anahtar verisi alanında taşınacak değerin uzunluğu 16' dan küçükse veya 16' dan büyük olup 8' in bir katı uzunluğunda değilse Anahtar verisi alanı dolgulanır. Dolgu alanında ilk sekizli (0xdd) olmalı ve eğer gerekli ise diğer dolgu sekizlileri (0x00) değeri ile dolgulanmalıdır.

Anahtar verisi alanında Grup anahtarı verisi veya STA anahtarı verisi taşınıyorsa fakat anahtar verisi alanı şifrelenmemiş ise bu paket işlenmemelidir.

Anahtar verisi alanında Grup anahtarı taşınması durumunda anahtar verisi alanında yer alacak veriye ilişkin format Şekil 4-10'da verilmiştir:



Şekil 4-10: EAPOL-Anahtar paketinde grup anahtarı taşınırken veri alanına yerleştirilecek format

Tx bayrağı kurulu ise bu EAPOL-Anahtar paketi içerisinde yer alana Grup anahtarı hem alım hem de gönderim amaçlı kullanılır. Tx bayrağı kurulu olmayan Grup anahtarı ile yalnızca alınan paketlerin şifresi çözülebilir, gönderimde şifreleme amaçlı kullanılamaz.

4.2 802.11i' de Kullanılan Kriptolojik Anahtar Hiyerarşisi ve Anahtar Dağıtımı

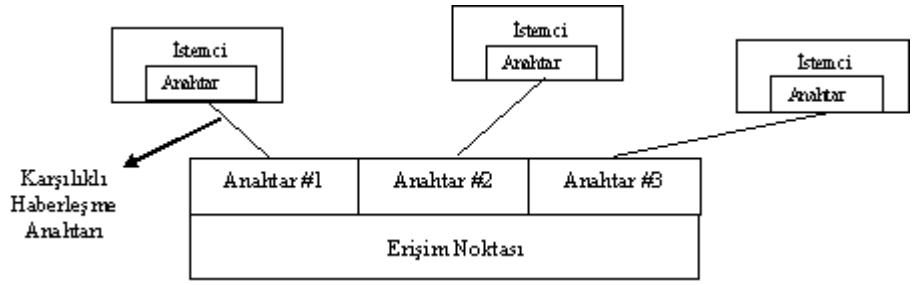
802.11i standardı WEP' in aksine farklı seviyelerde kullanılmak üzere farklı anahtarlar tanımlar ve kullanır. Gerek şifreleme işlemlerinde kullanılmak üzere gerekse bütünlük koruması değerlerinin hesaplanmasında kriptolojik anahtarlar kullanılır. Bu bölümde 802.11i standardının tanımladığı anahtar hiyerarşileri, oluşturulmaları ve dağıtımlarının ne şekilde yapıldığı incelenecektir.

4.2.1 Karşılıklı Haberleşme ve Grup Haberleşmesi

IEEE 802.11 ağları çeşitli ağ cihazlarının bir arada haberleşmeleri için tanımlanmıştır. Bu haberleşme sırasında karşılıklı bir çift cihaz birbiriyle (unicast) haberleşebileceği gibi bir cihaz birden fazla cihaz tarafından alınması gerekli mesajlar (multicast) da üretebilir. Bir cihaz tarafından üretilen ve diğer tüm cihazlara iletilmesi gereken mesajlar yayın (broadcast) mesajlarıdır ve çoğa-gönderimin (multicast) özel bir halidir.

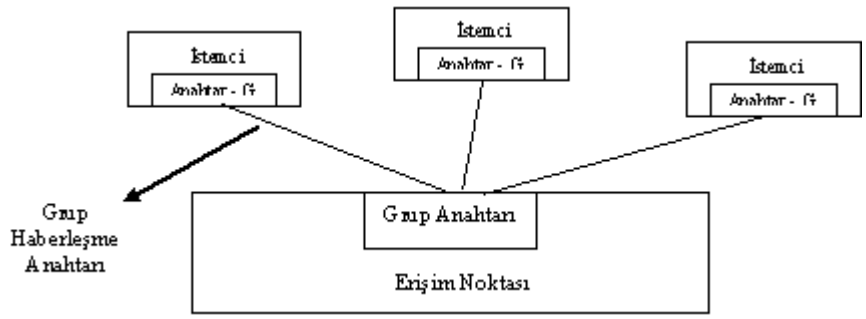
Karşılıklı haberleşme mesajlarının (unicast) yalnızca haberleşmede bulunan çiftler arasında özel olarak kalması, ortamda bulunan diğer cihazlar ve kişiler tarafından izlenemez olması gereklidir. 802.11i tarafından tanımlanan anahtar gruplarından ilki karşılıklı haberleşmenin korunmasını amaçlayan karşılıklı haberleşme anahtarıdır

(pairwise key). 802.11 ağları için alt yapılı çalışma modunda her istemcinin erişim noktasıyla haberleşmesinde kullanacağı bir adet karşılıklı haberleşme anahtarına sahip olması gerekir. Aksi taraftan ise erişim noktasının ortamda bulunan ve kendisiyle haberleşen her bir istemci için ayrı bir karşılıklı haberleşme anahtarına sahip olması gerekir. Erişim noktası her bir istemciyle ayrı ayrı haberleşirken farklı bir karşılıklı haberleşme anahtarı kullanır. Şekil 4-11 anlatılanları şekil üzerinde özetler:



Şekil 4-11: Karşılıklı haberleşme anahtarlarları gösterimi

Karşılıklı haberleşmenin aksine çoğa-gönderim paketlerinin birden fazla cihaz tarafından alınması ve anlaşılabilir olması gereklidir. Herhangi bir gruba üye olan kişiler arasındaki grup mesajları yalnızca bu gruba üye olanlar tarafından okunabilmeli ve ortamda bulunan fakat gruba üye olmayan cihaz ve kişilerin bu mesajları izleyemez olmaları gereklidir. 802.11i tarafından tanımlanmış ikinci anahtar grubu, çoğa-gönderim paketlerinin korunmasını amaçlayan grup anahtarıdır (group key). 802.11 ağları için alt yapılı çalışma modunda erişim noktasının grup anahtarı tektir ve bu anahtarı kendisiyle haberleşen tüm istemcilere çoğa-gönderim mesajlarının korunmasını sağlamak için gönderir. Şekil 4-12, grup anahtarı kullanımını şekil olarak ifade eder:



Şekil 4-12: Grup anahtarı gösterilimi

4.2.2 Karşılıklı Haberleşme Anahtarları Hiyerarşisi

Karşılıklı haberleşmede bulunan cihazların gönderip-aldıkları veri paketlerinin korunmasında karşılıklı haberleşme anahtarları kullanılır. Karşılıklı haberleşme anahtarları hiyerarşisinin temelinde 256 bitlik PMK anahtarı bulunur. PMK anahtarı önceden girilmiş bir ön paylaşımlı anahtar (PSK)' dan türetilebileceği gibi daha üst seviye karşılıklı kimlik doğrula işleminin sonucunda da üretilmiş olabilir.

Karşılıklı kimlik doğrulama işleminin 802.1X' in anlatıldığı bölümlerde EAP' protokolü ile gerçeklendiğini hatırlayalım. EAP üzerinde taşınacak kimlik doğrulama algoritmasının bir özelliğinin de kimlik doğrulama işleminin başarılı olması sonucunda rasgeleye yakın değerde bir anahtar üretebiliyor olması gerekir. 802.11i standardı bu tip kimlik algoritmalarının kullanılması gerektiğini belirtir fakat hangi kimlik doğrulama mekanizmasının kullanılacağını tanımlamaz. Örnek olarak ise TLS [18] veya Kerberos kimlik doğrulama mekanizmaları verilebilir. Kimlik doğrulama işlemi sonrasında istemci ve asıllama sunucusu tarafından üretilen ve asıllama sunucusundan asıllayıcıya gönderilen bu anahtara PMK anahtarı adı verilir.

Karşılıklı kimlik doğrulama işlemi için daha üst seviye bir kimlik doğrulama algoritması kullanılmaması durumunda PMK anahtarı doğrudan PSK' dan türetilir. PMK anahtarının boyu 256 bittir ve bu uzunlukta bir PSK girilmesi gerekli değildir. Bunun yerine 802.11i standardı daha kısa boydaki PSK' dan PMK anahtarının nasıl türetilebileceğini tanımlar [2]. Böylece kullanıcı daha kolay akılda kalabilen bir anahtar girerek haberleşmesini sağlayabilir.

Bahsi geçen iki yöntemden hangisinin tercih edileceği kullanıcıya bırakılmıştır. 802.11i standardı her iki kullanımı da destekler ve PSK girilmesi yöntemine daha basit olması ve bir asıllama sunucusu gerektirmemesinden dolayı "ev kullanımı" adını verir. Daha üst seviye bir kimlik doğrulama mekanizmasının (TLS, Kerberos, vb..) daha karmaşık bir alt yapı gerektirmesinden dolayı ise diğer yöntemi "profesyonel" olarak isimlendir. Her iki metodunda kendi artıları mevcuttur. PSK girilmesi daha basit ve zahmetsizken asıllama sunucusunun kullanılması tek elden yönetimi ve ölçeklenebilirliği arttırır. PSK anahtarının paylaşılan istemcilerde saklı kalması ve herhangi bir başkası tarafından öğrenilmemesi durumunda güvenlik açısından herhangi bir farkları yoktur.

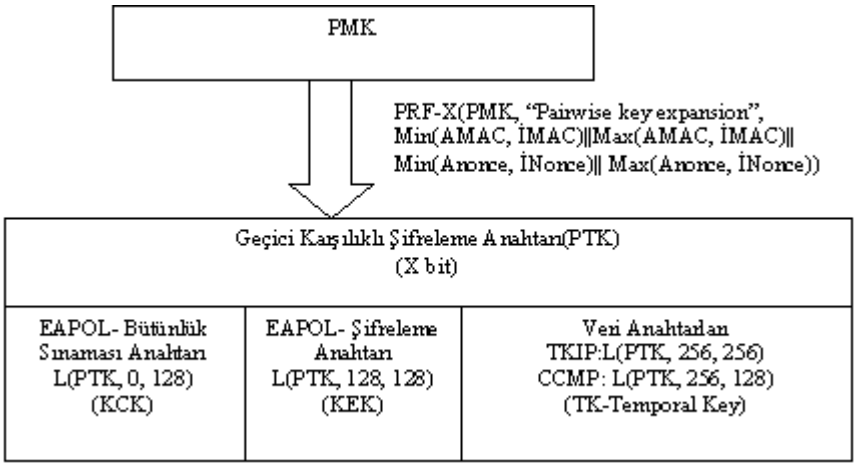
Her iki durumda da üretilecek PMK doğrudan veri trafiğinin korunmasında kullanılmaz. Bunun yerine PMK anahtarı iki cihazın haberleşmesini güvenli yapabilmeleri için gerekli 4 anahtarın üretilmesinde kullanılır. Bu 4 anahtarın hepsine birden geçici karşılıklı haberleşme anahtarı adı verilir (PTK-Pairwise Transient Key). Bu anahtarlar geçicidir ve her haberleşme birliği kurulmasında yeniden üretilir. Üretilmesi gereken bu 4 anahtar şunlardır:

- EAPOL-Anahtar Şifreleme Anahtarı (128 bit)-(KEK)
- EAPOL-Anahtar Bütünlük Sınaması Anahtarı (128 bit)-(KCK)
- Veri Şifreleme Anahtarı
- Veri Bütünlük Sınaması Anahtarı

Yukarıda verilen 4 anahtardan EAPOL anahtarları 4-yollu el sıkışma mekanizmasında, grup anahtarı dağıtımı sırasında ve gerektiğinde diğer EAPOL mesajlarının korunmasında kullanılır. Veri şifreleme ve bütünlük sınaması anahtarları ise haberleşen iki cihaz arası veri trafiğinin korunmasında kullanılır ve kullanılacak algoritmaya göre farklı uzunluktadırlar. PTK' nın üretilmesi için gerekli diğer parametreler 4-yollu el sıkışma işlemi sırasında üretilir ve değiş-tokuş edilir. PMK dışındaki bu değerler şunlardır:

- İNonce: İstemci tarafından üretilen rasgele sayı (32 sekizli)
- ANonce: Asıllayıcı tarafından üretilen rasgele sayı (32 sekizli)
- İMAC: İstemciye ait MAC adresi (6 sekizli)
- AMAC: Asıllayıcıya ait MAC adresi (6 sekizli)

Tüm bu değerlerden PTK' nın üretilmesi ve PTK' nın kullanılacak 4 anahtara bölümlenmesi Şekil 4-13'de gösterilmiştir:



Şekil 4-13: Karşılıklı haberleşme anahtarları hiyerarşisi

Min(A,B): işlemi A ve B sayılarından en küçük olanını seçer.

Max(A,B): işlemi A ve B sayılarından en büyük olanını seçer.

A||B: işlemi B dizisinin, A dizisinin arkasına ekleneceğini ifade eder.

L(X, i, u): işlemi X bit dizisinde i. bitten başlanarak u bit alınacağını ifade eder.

PRF-X(...): işlemi Sözde Rasgele Fonksiyonunu(PRF-Pseudo-Random Function) ifade eder.

802.11 ağında veri haberleşmesinin güvenliğinin sağlanması için TKIP algoritması kullanılacaksa Veri anahtarları alanının ilk 128 biti şifreleme anahtarı olarak son 128 biti bütünlük sınaması anahtarı olarak kullanılır. Yani simgesel gösterilimi kullanacak olursak:

- $TKIP_{şifreleme} = L(PTK, 256, 128)$
- $TKIP_{özet} = L(PTK, 384, 128)$

802.11 ağında veri haberleşmesinin güvenliğinin sağlanması için CCMP algoritması kullanılacaksa, algoritmanın doğası gereği aynı anahtarla şifreleme yapılır ve bütünlük özeti değeri hesaplanır. Veri anahtarı alanının ilk 128 biti hem şifreleme işleminde hem de özet değerinin hesabında kullanılır. Yani simgesel gösterilimi kullanacak olursak:

- $CCMP_{şifreleme/özet} = L(PTK, 256, 128)$

4.2.3 Grup Anahtarları Hiyerarşisi

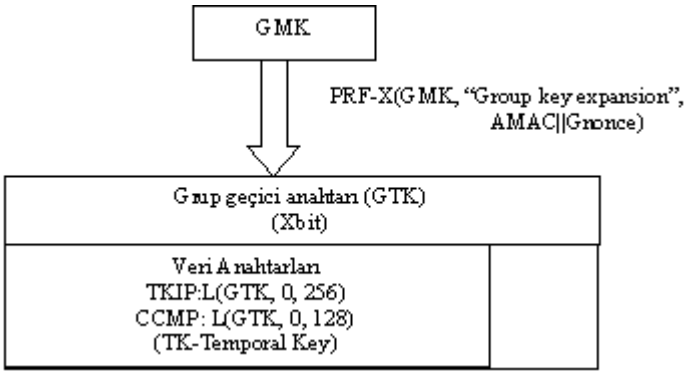
802.11 ağları paylaşılan ağlardır ve birden fazla cihaz tarafından alınması istenilen çoğa-gönderim (multicast) paketleri kullanılabilir. Herhangi bir gruba üye olan kişiler arasındaki grup mesajları yalnızca bu gruba üye olanlar tarafından okunabilmeli ve ortamda bulunan fakat gruba üye olmayan cihaz ve kişilerin bu mesajları izleyemez olmaları gereklidir. Bu amaçla karşılıklı haberleşme anahtarları kullanılamaz, çünkü her bir istemcinin anahtarı farklı olacaktır. Çoğa-gönderim paketlerinin korunması için 802.11i standardı grup anahtarları hiyerarşisini tanımlar. Grup anahtarları hiyerarşisinde karşılıklı haberleşme anahtarlarının aksine tüm istemciler aynı ortak anahtarları paylaşırlar. Alt yapılı 802.11 ağlarında bu anahtarı erişim noktası belirler ve kendisi ile haberleşme birliği (association) kurmuş olan tüm istemcilere gönderir. Alt yapısız rast-gele yapılı 802.11 ağlarında ise her bir istemcinin kendisine ait bir grup anahtarı söz konusudur. Bu durumda her istemci kendisi ile haberleşen diğer tüm istemcilere kendi grup anahtarını gönderir.

Alt yapılı çalışma modunda istemciler kendilerine gönderilmiş grup anahtarını kullanarak çoğa-gönderim mesajlarını şifreleyip gönderemezler. Bunun yerine çoklu yayın yapılması gereken paketi önce erişim noktasına gönderirler. Daha sonra erişim noktası bu paketi grup anahtarıyla kapatarak diğer tüm istemcilere gönderir [12].

Gruba üye bir istemci ayrılmak istediği zaman bu istemciye ait karşılıklı anahtar silinir ve bu istemciye artık veri gönderilmez. Ayrılan istemcinin artık gruba üye olmadığı ve gruba ait grup anahtarını bildiğini göz önüne alırsak mevcut grup anahtarının güncellenmesi gerekecektir. Aksi takdirde gruba üye olmayan bir istemcinin gruba ait mesajları izlemesine olanak verilmiş olunur.

Grup anahtarları karşılıklı haberleşme anahtarı oluşturulduktan sonra bu anahtar kullanılarak şifrelenir ve istemcilere EAPOL-Anahtar paketi ile gönderilir. Grup anahtarı değişimi mekanizması bu nedenle daha basittir ve 2-yollu el sıkışma mekanizması olarak adlandırılan metotla istemcilere gönderilir.

Grup anahtarları hiyerarşisinin temelinde 256 bitlik GMK anahtarı bulunur. GMK asıllayıcı (alt yapılı 802.11 çalışma modu için erişim noktası) tarafından rasgele olacak şekilde 256 bit olarak üretilir. Daha sonra GMK' dan grup haberleşmesinde kullanılacak geçici anahtar olan GTK anahtarı üretilir. Buna ilişkin mekanizma Şekil 4-14'de verilmiştir:



Şekil 4-14: Grup anahtarı hiyerarşisi

802.11 ağında grup haberleşmesinin güvenliğinin sağlanması için TKIP algoritması kullanılacaksa Veri anahtarları alanının ilk 128 biti şifreleme anahtarı olarak son 128 biti bütünlük sınaması anahtarı olarak kullanılır. Yani simgesel gösterilimi kullanacak olursak:

- $GTKIP_{şifreleme} = L(PTK, 256, 128)$
- $GTKIP_{özet} = L(PTK, 384, 128)$

802.11 ağında grup haberleşmesinin güvenliğinin sağlanması için CCMP algoritması kullanılacaksa Veri anahtarı alanının ilk 128 biti hem şifreleme işleminde hem de özet değerinin hesabında kullanılır. Yani simgesel gösterilimi kullanacak olursak:

- $GCCMP_{şifreleme/özet} = L(PTK, 256, 128)$

GMK' nın rasgele seçildiğinden dolayı GTK' nın hesaplanmasının gereksiz gibi durmaktadır. Fakat bu hesaplama karşılıklı haberleşme anahtarlarının oluşturulması ile bir tutarlılık sağlamak amaçlı olduğu düşünülebilir.

4.3 Dört-yollu El Sıkışma Mekanizması

802.11 haberleşmesinin kurulması için 802.1X ve EAP kullanılarak karşılıklı kimlik doğrulama işlemi uygulandığında istemci ve asıllama sunucusu birbirlerini doğrulamış olurlar. Bu haberleşmede güvenlik bakımından eksik kalan nokta istemci ile asıllayıcının birbirini doğrulamamış olmasıdır, çünkü asıllayıcı EAP paketlerinin taşınması için istemci ile asıllama sunucusu arasında bir köprü görevi görmüş ve karşılıklı kimlik doğrulama işleminde başka herhangi bir katkıda bulunmamıştır. Bu

nedenle istemcinin haberleşeceği asıllayıcıyı doğrulaması, asıllama sunucusu tarafından asıllayıcıya gönderilmiş olması gereken PMK anahtarının asıllayıcıdaki varlığını ve bu anahtarın istemcinin sahip olduğu anahtarla aynı olduğunu görmesi gereklidir.

İstemcinin, asıllayıcıyı doğrulaması için asıllayıcıda olması gereken PMK anahtarının kendi ürettiği PMK anahtarı ile aynı olduğunu görmesi yeterli olacaktır. Çünkü asıllayıcıda istemcinin sahip olduğu PMK anahtarının aynısının olması ancak ve ancak asıllama sunucusunun bu anahtarı asıllayıcıya göndermiş olmasıyla mümkün olacaktır. Asıllama sunucusu istemci ile karşılıklı ürettiği PMK anahtarını asıllayıcıya göndererek, asıllayıcıya duyduğu güveni ifade eder. Eğer asıllama sunucusu asıllayıcıya güveniyorsa istemcide asıllayıcıya güvenmek durumundadır, çünkü kurulmuş güvenlik mimarisinin temelinde asıllama sunucusu yer alır. Benzer şekilde asıllama sunucusunun güvenmiş olduğu istemcideki PMK anahtarının kendisine gönderilen PMK anahtarı ile aynı olduğunu görmek asıllayıcı için istemcinin güvenilir olduğu anlamına gelecektir.

802.11i' de tanımlı olan 4-yollu el sıkışma mekanizması karşılıklı doğrulama mekanizmasının son adımlarını oluşturur ve asıllayıcı ile istemcinin birbirini doğrulamasını sağlar. 4-yollu el sıkışma mekanizması EAPOL-Anahtar mesajları kullanılarak gerçekleştirilir. Sadece asıllayıcı tarafından başlatılan ve EAPOL-Anahtar mesajlarının kullanıldığı 4-yollu el sıkışma mekanizmasının amacı şunlardır:

- Kullanıcının PMK' yı oluşturduğundan emin olmak
- PMK' nın güncel olduğundan emin olmak
- PMK' yı kullanarak PTK' yı oluşturmak
- Karşılıklı şifreleme ve bütünlük kontrolü anahtarlarının yüklenmesini sağlamak
- Erişim noktasının oluşturduğu Geçici Grup Anahtarını (GTK-Group Transient Key) kullanıcıya aktarmak

4-yollu el sıkışma mekanizmasında öncelikle istemci ve asıllayıcı tarafından daha önce kullanılmamış rasgele sayılar üretilmesiyle başlanır. 32 sekizlilik bu rasgele sayılara "**nonce**" adı verilir. İngilizce bir kelime olan "nonce", "n-once" olarak yazıldığında daha anlamlı bir ifade elde edilmiş olunur, yani sadece tek kullanımlık

bir sayı anlamını ifade eder. Aynı PMK anahtarı ve MAC adresi için sadece bir defa kullanılacak ve daha önceden tahmin edilemeyen bir değerin üretilmesi gerekir. Gerçek rasgele sayıların üretilmesindeki zorluk göz önüne alınarak 802.11i standardında "nonce" değerlerinin nasıl üretilebileceğine dair örnek verilmiştir:

nonce = PRF-256(Rasgele Sayı, "Init Counter", MAC || zaman)

Rasgele Sayı: Cihaz tarafından üretilebilecek en iyi rasgele sayıyı ifade eder.

MAC: Rasgele sayıyı üretecek cihazın MAC adresini ifade eder.

Zaman: Rasgele sayıyı üretecek cihazın zamanı ("Network Time") ifade eder.

İstemci tarafından üretilecek "nonce" değerini İNonce, asıllayıcı tarafından üretilecek "nonce" değerini ANonce olarak isimlendirelim. Bu aşamadan sonra asıllayıcı tarafından başlatılan , 4 mesajın gönderilip alındığı ve EAPOL-Anahtar paketlerinin kullanıldığı mekanizma yürütülür.

Mesaj(A): Asıllayıcı → İstemci

4-yollu el sıkışma mekanizmasının ilk mesajı her zaman asıllayıcı tarafından üretilir ve istemciye gönderilir. Asıllayıcının gönderdiği ilk mesajın içerisinde asıllayıcı tarafından üretilmiş ANonce değeri yer alır. Bu ilk mesaj şifrelenmez ve bütünlük sınaması hesaplanmaz. Mesajın yolda değiştirilmesi sadece 4-yollu el sıkışma işleminin başarısızlıkla sonuçlanmasına yol açacaktır, güvenlik açısından bir sorun oluşturmaz.

İstemci bu ilk mesajı aldığında geçici karşılıklı haberleşme anahtarını (PTK) oluşturması için gerekli tüm bilgilere sahip olmuş olur. PMK anahtarını, kendi ürettiği İNonce değerini, kendi MAC adresini (İMAC) bilen istemci, aldığı mesajdan da ANonce değerini ve asıllayıcının MAC adresini (AMAC) öğrenir ve PTK anahtarını oluşturur.

Mesaj(B): İstemci → Asıllayıcı

Asıllayıcı PTK anahtarını oluşturmak için gerekli tüm bilgilere henüz sahip değildir, istemci tarafından üretilen İNonce değerini bilmemektedir. İstemci kendi üretmiş olduğu İNonce değerini ikinci mesajla asıllayıcıya iletir. Bu istemci tarafından asıllayıcıya gönderilen ikinci mesaj da şifrelenmez, fakat ilk mesajın aksine bütünlük

sınaması hesaplanır. Bütünlük sınamasının hesabında kullanılan anahtarın ne olduğu karşılıklı haberleşme anahtarları hiyerarşisi bölümünde anlatılmıştır. Gönderilen EAPOL-Anahtar paketinin tamamı üzerinden hesaplanan bütünlük sınaması, paketin yolda değiştirilmemiş olduğunu garanti eder, ayrıca asıllayıcıya istemcinin PMK anahtarını bildiğini ispat etmiş olur. Aldığı ikinci paketten İNonce değerini okuyan asıllayıcı artık PTK' yı hesaplamak için gerekli tüm bilgilere sahip olmuş olur. asıllayıcının PTK' yı oluşturduktan sonra gelen mesajın bütünlük sınaması değerini aynen hesaplayabiliyor olması, asıllayıcıya istemcinin PTK' yı dolayısıyla PMK' yı bildiğini ve kimliğini ispatlamış bir kullanıcı olduğunu ispat eder.

Bu aşamada yolun yarısı tamamlanmış, karşılıklı taraflarda PTK' lar hesaplanmış ve asıllayıcıya istemcinin kimliği kanıtlanmış olunur. Her iki tarafta PTK' yı hesaplamış olsalar da şifreleme işlemi henüz başlatılmaz.

Mesaj(C): Asıllayıcı → İstemci

Asıllayıcıdan istemciye gönderilen bu mesaj istemciye oluşturulan PTK anahtarının kullanılmaya hazır olduğunu bildirir. Durum senkronizasyonu sağlanmaz ise ve herhangi bir taraf diğerinden önce şifreleme başlarsa bağlantı kopmuş sayılır. Asıllayıcının gönderdiği bu üçüncü mesaj da şifrelenmez, fakat bütünlük sınaması değeri hesaplanır. Bütünlük sınaması değerinin istemci tarafından aynı olarak hesaplanması istemciye hem paketin yolda değişmemiş olduğunu hem de asıllayıcının doğru PTK' ya dolayısıyla doğru PMK' ya sahip olduğunu göstermiş olur. Asıllayıcının doğru PMK' ya sahip olması asıllama sunucusunun asıllayıcıya güvendiğini dolayısıyla istemcinin de asıllayıcıya güvenebileceğini istemciye ispat etmiş olur.

Üçüncü mesajın içerisinde ayrıca istemcinin veri şifrelemede kullanacağı sıra numarası başlangıç değerini de gönderilir (genelde sıfır).

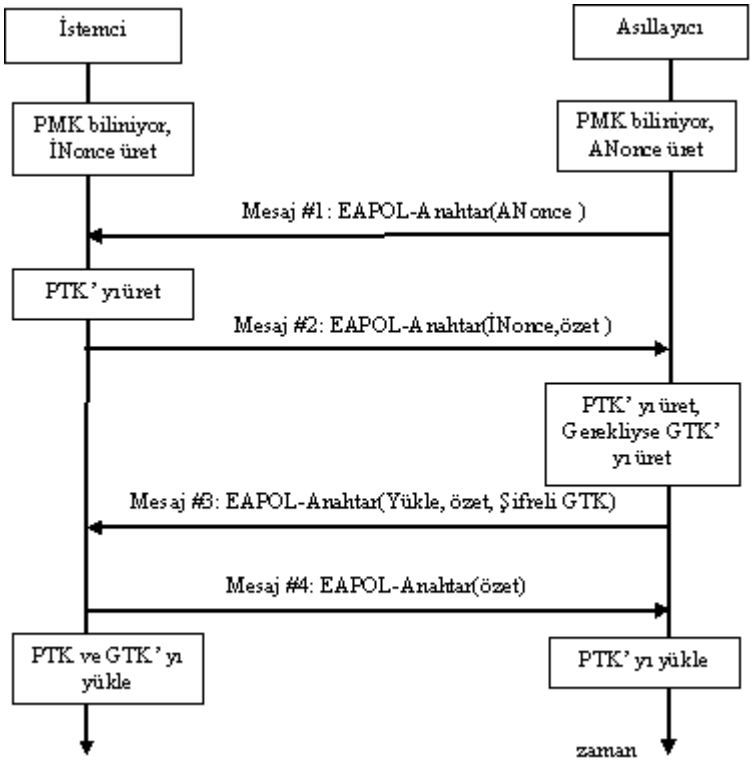
Mesaj(D): İstemci → Asıllayıcı

Bu yanıt mesajı 4-yollu el sıkışma mekanizmasının tamamlandığını ve istemcinin bundan sonra veri mesajlarını şifrelemeye başlayacağını bildirir. Mesaj şifrelenmeden gönderildikten sonra istemci veri mesajlarının korunması için üretilen PTK anahtarlarını kullanmaya başlar. 4. mesajı alan asıllayıcı da mesajı aldıktan sonra 4-yollu el sıkışma mekanizmasının başarıyla tamamlandığını anlar ve veri mesajlarının korunması için üretilen PTK anahtarlarını kullanmaya başlar.

4-yollu el sıkışma sırasında başarılmış adımları gözden geçirirsek:

- ANonce ve İNonce değerleri başarıyla karşı tarafa aktarılmıştır.
- İstemci PMK anahtarını doğru olarak bildiğini ispatlamıştır.
- Asıllayıcı PMK anahtarını doğru olarak bildiğini ispatlamıştır.
- Geçici haberleşme anahtarları (PTK) hesaplanmıştır.
- Her iki cihazda senkronize olmuş ve veri paketlerinin şifrelenmesine başlanılmıştır.

4-yollu el sıkışma mekanizması şekil olarak Şekil 4-15'de verilmiştir:



Şekil 4-15: 4-yollu el sıkışma mekanizması

4-yollu el sıkışma sırasında kullanılan EAPOL-Anahtar mesajlarının yapıları için bir simgesel gösterilim oluşturacak olursak:

EAPOL-Anahtar(G, Ö, C, Y, T, ASN, ANonce/İNonce, Özet, RSN-BE, GTK)

- G: EAPOL-Anahtar paketlerinde yer alan güvenli bayrağını ifade eder.
- Ö: EAPOL-Anahtar paketinde özet bilgisinin (bütünlük sınaması değeri) yer alıp almadığını ifade eder.

- C: Gönderilen EAPOL-Anahtar paketine istinaden bir cevap gönderilip gönderilmeyeceğini ifade eder.
- Y: Oluşturulacak olan PTK anahtarının yüklenip kullanılmaya başlanıp başlanmayacağını ifade eder.
- T: EAPOL-Anahtar paketleri ile oluşturulacak anahtarın tipini ifade eder.
    - K: Karşılıklı haberleşme anahtarı
    - G: Grup anahtarı
- ASN: EAPOL-Anahtar paketlerinde yer alan Alınan Sıra Numarası değerini ifade eder.
- ANonce/İNonce: Asıllayıcı rasgele sayısı/ İstemci rasgele sayısını ifade eder.
- Özet: EAPOL-Bütünlük Sınaması Anahtarı kullanılarak oluşturulan özet değerini ifade eder.
- RSN-BE: 802.11i standardında tanımlanan güvenlik bilgi elemanını ifade eder.
- GTK: Grup anahtarını ifade eder.

4-yollu el sıkışma mekanizmasında kullanılan mesajların tanımlanmış simgesel gösterilimi aşağıdaki gibi olacaktır:

- Mesaj #1 Asıllayıcı → İstemci

  EAPOL-Anahtar(0, 0, 1, 0, K, 0, ANonce, 0, 0, 0)

- Mesaj #2 İstemci → Asıllayıcı

  EAPOL-Anahtar(0, 1, 0, 0, K, 0, İNonce, özet, RSN-BE, 0)

- Mesaj #3 Asıllayıcı → İstemci

  EAPOL-Anahtar(1, 1, 1, 1, K, ASN, ANonce, özet, RSN-BE, GTK)

- Mesaj #4 İstemci → Asıllayıcı

  EAPOL-Anahtar(1, 1, 0, 0, K, 0, 0, özet, 0, 0)

4.4 İki-yollu El Sıkışma Mekanizması

IEEE 802.11 haberleşmesi yayın ve çoğa-gönderim mesajlarını destekler. Çoğa-gönderim paketlerinin korunması için 802.11i standardı grup anahtarlarını tanımlar. Grup anahtarları hiyerarşisinde karşılıklı haberleşme anahtarlarının aksine tüm istemciler aynı ortak anahtarları paylaşırlar. Grup anahtarları karşılıklı haberleşme anahtarı oluşturulduktan sonra bu anahtar kullanılarak şifrelenir ve istemcilere EAPOL-Anahtar paketi ile gönderilir. Grup anahtarı değişimi mekanizması bu nedenle daha basittir ve 2-yollu el sıkışma mekanizması ile grup anahtarı değişimi kotarılabilir.

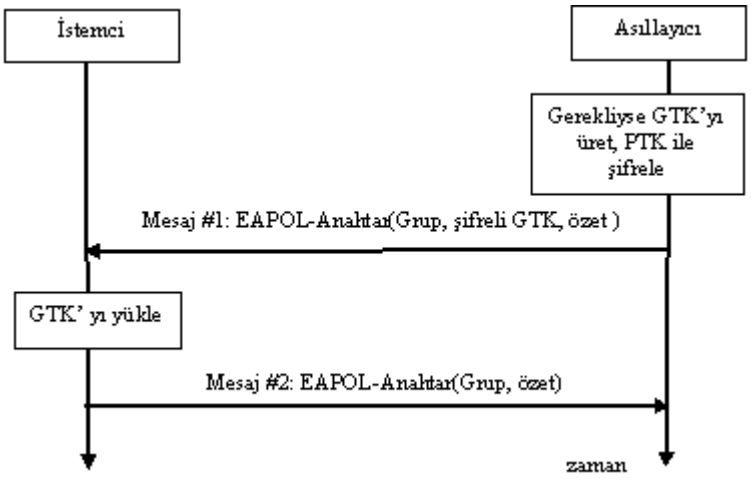
Mesaj(A): Asıllayıcı → İstemci

Asıllayıcı kendisine ait olan GTK anahtarını üretir, EAPOL-Anahtar paketine yerleştirir ve göndereceği istemciyle paylaştığı PTK anahtarıyla EAPOL-Anahtar paketini kapatır. Bütünlük sınaması değerini hesaplar ve paketin içine yazarak paketi istemciye gönderir. İstemci sahip olduğu PTK anahtarları yardımıyla gelen paketin bütünlük sınaması kontrolünü yaptıktan sonra eğer bütünlük kontrolü başarılıysa EAPOL-Anahtar paketini PTK yardımıyla çözer ve grup haberleşmesinde kullanılacak GTK anahtarına sahip olmuş olur.

Mesaj(B): İstemci → Asıllayıcı

İstemci GTK anahtarını başarıyla aldığı bilgisini oluşturur ve EAPOL-Anahtar paketi içerisinde asıllayıcıya gönderir. Herhangi bir veri yerleştirilmek zorunda değildir. Paketin bütünlük sınaması PTK anahtarları yardımıyla hesaplanır ve pakete konulur. İstemci aldığı mesajın bütünlük sınamasını doğru olarak yaparsa istemcinin GTK anahtarını almış olduğunu anlar.

2-yollu el sıkışma mekanizması şekil olarak Şekil 4-16'da verilmiştir:



Şekil 4-16: Grup anahtarı el sıkışması

2-yollu el sıkışma mekanizmasında kullanılan mesajların tanımlanmış simgesel gösterilimi aşağıdaki gibi olacaktır:

- Mesaj #1 Asıllayıcı → İstemci

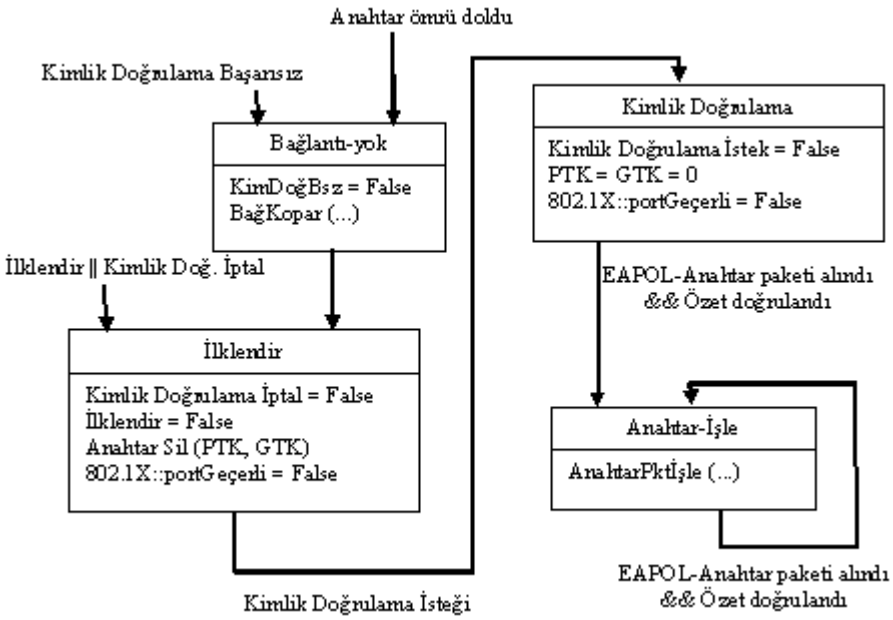
  EAPOL-Anahtar(1, 1, 1, 0, G, ASN, 0, özet, 0, GTK)

- Mesaj #2 İstemci → Asıllayıcı

  EAPOL-Anahtar(1, 1, 0, 0, G, 0, 0, özet, 0, 0)

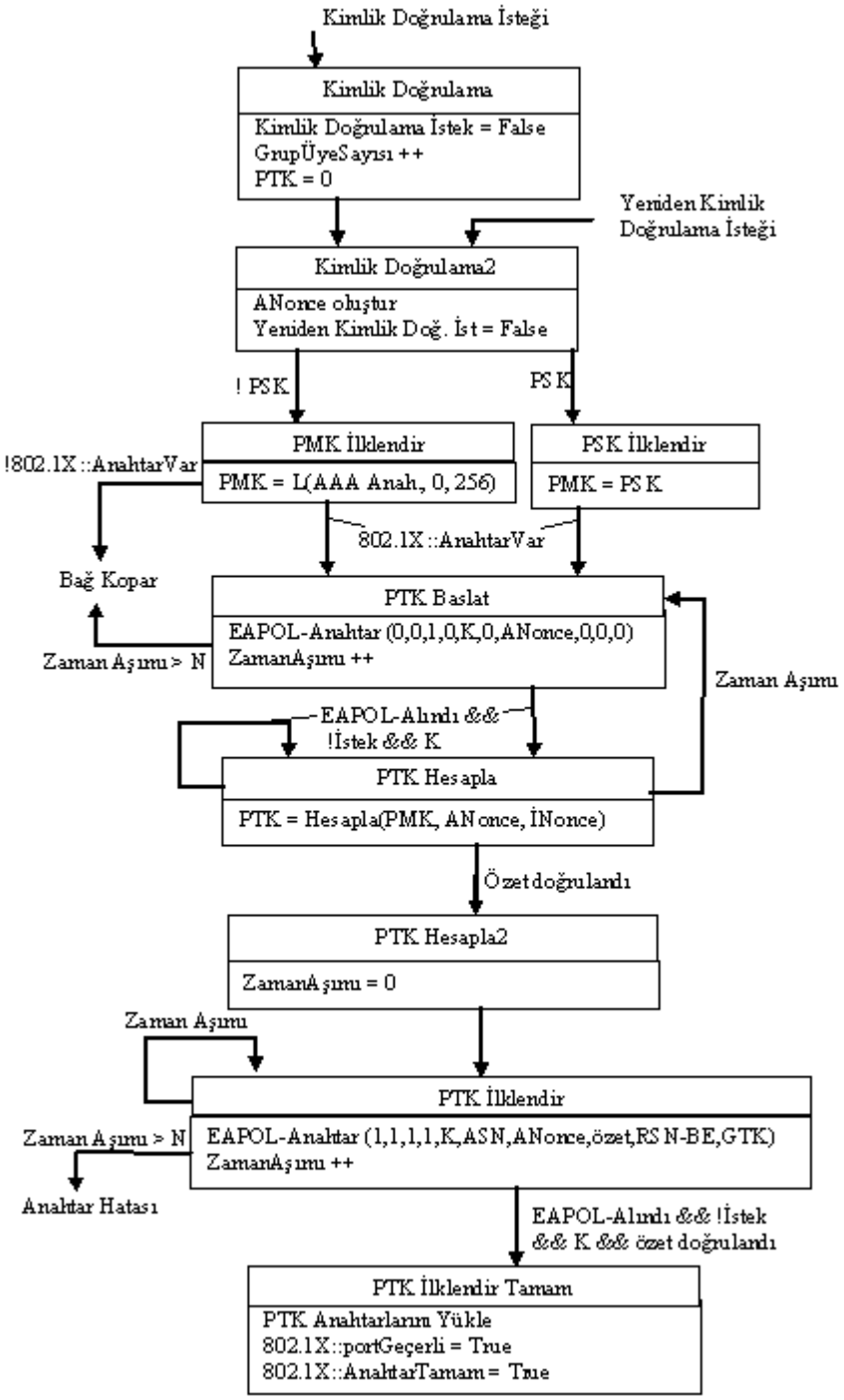
4.5 İstemci Anahtar Yönetimi Durum Makinesi

İstemci anahtar yönetimi sonlu durum makinesi zaman aşımı ve tekrar gönderim işlemleri gerçekleştirmez. Oldukça basit olan istemci anahtar yönetimi durum makinesi Şekil 4-17'deki gibi verilebilir:

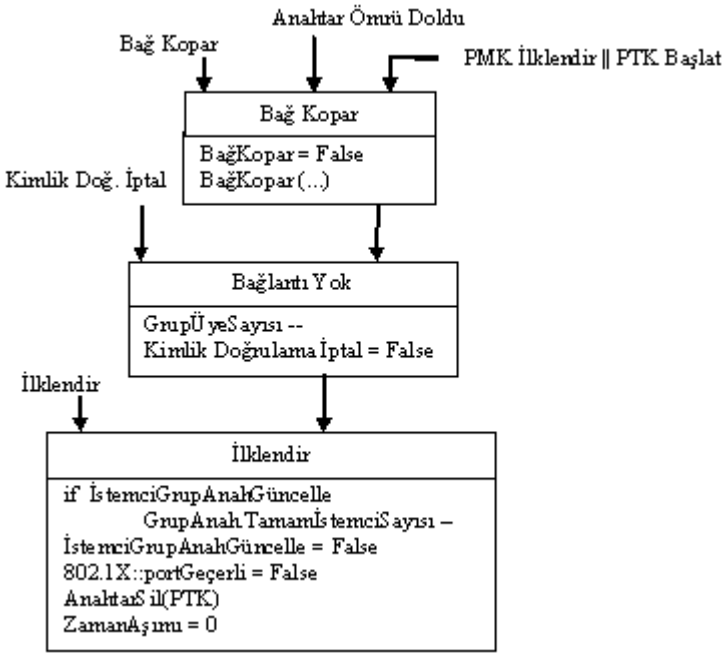


Şekil 4-17: İstemci anahtar yönetimi sonlu durum makinesi

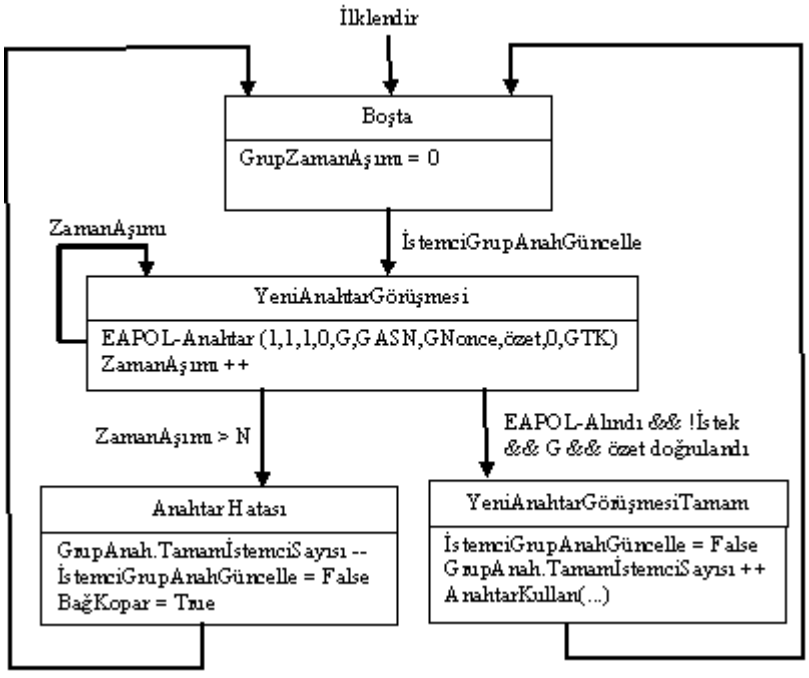
4.6 Asıllayıcı Anahtar Yönetimi Durum Makinesi



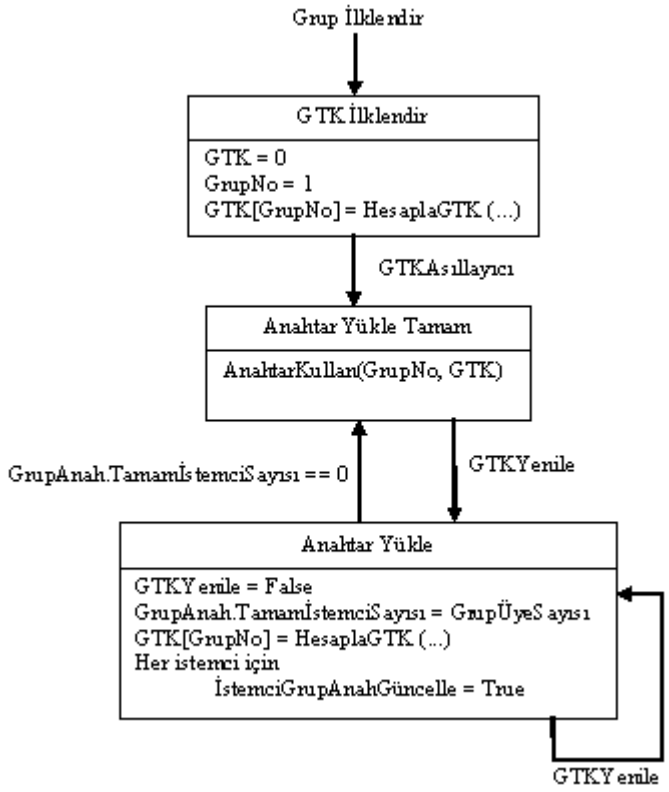
Şekil 4-18: Asıllayıcı anahtar yönetimi durum makinesi bölüm#1



Şekil 4-19: Asıllayıcı anahtar yönetimi durum makinesi bölüm#2



Şekil 4-20: Asıllayıcı anahtar yönetimi durum makinesi bölüm#3

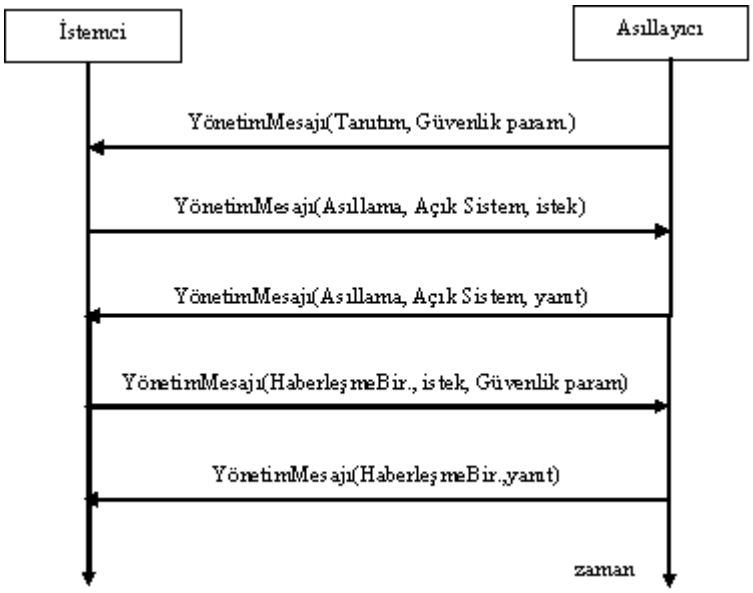


Şekil 4-21: Asıllayıcı anahtar yönetimi durum makinesi bölüm#4

4.7 802.11i' de haberleşmeye geçiş adımları

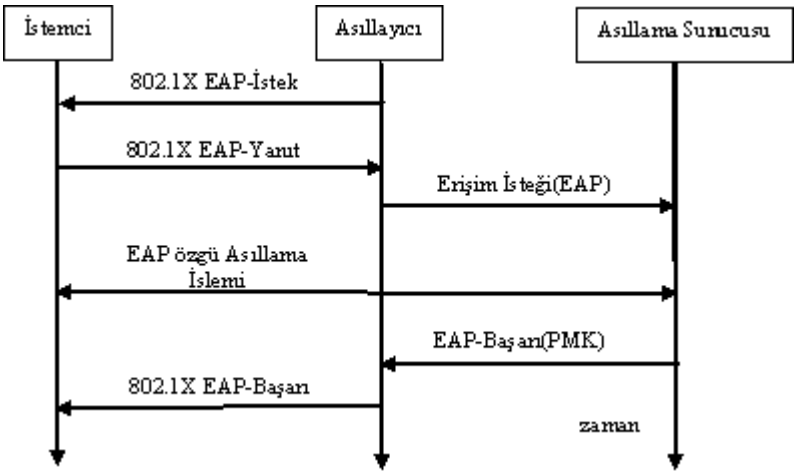
Yeni kimlik doğrulama ve anahtar oluşturulması için el sıkışma mekanizmaları tanımlandığından 802.11i' de haberleşmeye geçiş aşamaları 802.11-1999 standardına göre farklıdır. Yeni açılan bir istemcinin ortamdaki erişim noktalarını bulup onlarla haberleşmeyi kurmasına kadar geçen aralıkta gerçekleştirilen adımlar aşağıda verilmiştir:

- Kullanıcı, erişim noktasının uyguladığı güvenlik mekanizmalarının neler olduğunu erişim noktası tanıtım paketlerini dinleyerek veya erişim noktası sorgusunu kullanarak öğrenir.
- Erişim denetimi mekanizması koşturulmadan önce kullanıcı ve erişim noktası arasında haberleşme birliği (association) kurulmalıdır. Bu iki adım Şekil 4-22'de verilmiştir:



Şekil 4-22: Haberleşmeye geçiş, haberleşme birliğinin kurulması

- Bu aşamadan sonra eğer 802.1X erişim denetimi kullanılıyor ise EAP kimlik doğrulama mekanizması erişim noktasının göndereceği EAP-İstek paketiyle veya kullanıcının göndereceği EAPOL-Başlat mesajı ile başlatılır. EAP kimlik doğrulama paketleri asıllayıcı ile asıllama sunucusu arasındaki haberleşme yolunun güvenli olduğu varsayımı altında, kullanıcı ile asıllama sunucusu arasında, asıllayıcının kontrolsüz portu kullanılarak gönderilip-alınır.
- Seçilen EAP kimlik doğrulama algoritması sonucunda kullanıcının ağa erişim yetkisinin olup olmadığı kararını asıllama sunucusu verir ve bu kararı asıllayıcıya iletilir. Kimlik doğrulama işleminin başarılı olması durumunda kullanıcı ve asıllama sunucusu Karşılıklı Ana Anahtar (PMK-Pairwise Master Key) oluştururlar. Asıllama sunucusu bu anahtarı güvenli kabul edilen haberleşme kanalı üzerinden asıllayıcıya gönderir. 802.1X asıllama adımları Şekil 4-23' de gösterilmiştir:



Şekil 4-23: IEEE 802.1X EAP Asıllama

- Bu aşamada asıllayıcının kullanıcıya ilişkin kontrollü portu hala aktif edilmemiştir. Son olarak kullanıcı ile asıllayıcı arasındaki veri haberleşmesinin güvenliğini sağlayacak karşılıklı geçici anahtar (PTK-Pairwise Transient Key) kullanıcı ile asıllayıcı arasında 4-yollu el sıkışma mekanizması ve PMK kullanılarak oluşturulur.

  Sadece asıllayıcı tarafından başlatılan ve EAPOL-Key mesajlarının kullanıldığı 4-yollu el sıkışma mekanizmasının amacı şunlardır:

  - Kullanıcının PMK' yı oluşturduğundan emin olmak
  - PMK' nın güncel olduğundan emin olmak
  - PMK' yı kullanarak PTK' yı oluşturmak
  - Karşılıklı şifreleme ve bütünlük kontrolü anahtarlarının yüklenmesini sağlamak
  - Erişim noktasının oluşturduğu Geçici Grup Anahtarını (GTK-Group Transient Key) kullanıcıya aktarmak

Asıllayıcı tarafından 802.1X kullanılmayabilir. 802.1X kimlik doğrulama mekanizması 802.11i standardı için seçime bağlıdır. 802.1X kullanılmaması durumunda karşılıklı kimlik doğrulama ön paylaşımlı anahtarla (PSK-PreShared Key) yapılır. 4-yollu el sıkışma mekanizmasında kullanılacak olan PMK anahtarı PSK' dan türetilir.

5 TKIP

802.11i-2004 standardında hali hazırda kullanılmakta olan telsiz yerel bilgisayar ağları ekipmanlarında donanım değişikliği gerektirmeden yazılım güncellemesiyle çalıştırılabilecek güvenlik mekanizmaları da ele alınmış ve bu amaçla TKIP (Temporal Key Integrity Protocol-Geçici Anahtar Bütünlüğü Protokolü) standarda konulmuştur. TKIP protokolü temelde WEP kapsüllemesini kullanmasına karşın WEP protokolü üzerinde bir çok değişiklik tanımlayarak bilinen pasif ve aktif saldırılara karşı koyabilecek yapıdadır.

TKIP protokolü 802.11i standardı için gerçekleştirilmesi zorunlu bir protokol değildir, ancak mevcut donanımlar üzerinde çalışabilmesi açısından WEP' ten 802.11i standardına yumuşak geçişin sağlanması amaçlanmıştır. Öncelikle mevcut cihazlar TKIP kullanabilir hale getirilecek zaman içerisinde 802.11i' nin tanımladığı yeni güvenlik mekanizmalarını kullanan cihazlar üretildikçe TKIP kullanan cihazlar kullanımdan kaldırılabilecektir. Geçiş protokolü olarak düşünülmesi TKIP tasarlanırken göz önüne alınması gereken iki maddeyi beraberinde getirir. TKIP hem mevcut cihazlar üzerinde koşabilecek kadar yalın olmalı, mümkünse aynı şifreleme yöntemini kullanabilmeli ve de güvenliği sağlayacak kadar güçlü olmalıdır.

5.1 TKIP Protokolüne Genel Bakış

Daha önceki bölümlerde de ele alındığı gibi WEP protokolü bir çok yönden eksiklikler ve zayıflıklar gösterir. Başlıca problemler Tablo 5-1'de verilmiştir:

Tablo 5-1: WEP protokolü zayıflıkları

1	IV alanı çok kısadır ve kısa sürede tekrarlanan IV değerleri kullanılmaya başlanır
2	IV değerinin anahtarın başına eklenmesiyle oluşturulan RC4 ilklendirme değeri zayıf anahtarların oluşmasına dolayısıyla anahtarın ele geçirilmesine yol açan saldırılara yol açar
3	Mesaj veri bütünlüğü için etkin bir koruma yoktur
4	Mesaj tekrarlarına karşı bir savunma mekanizması yoktur

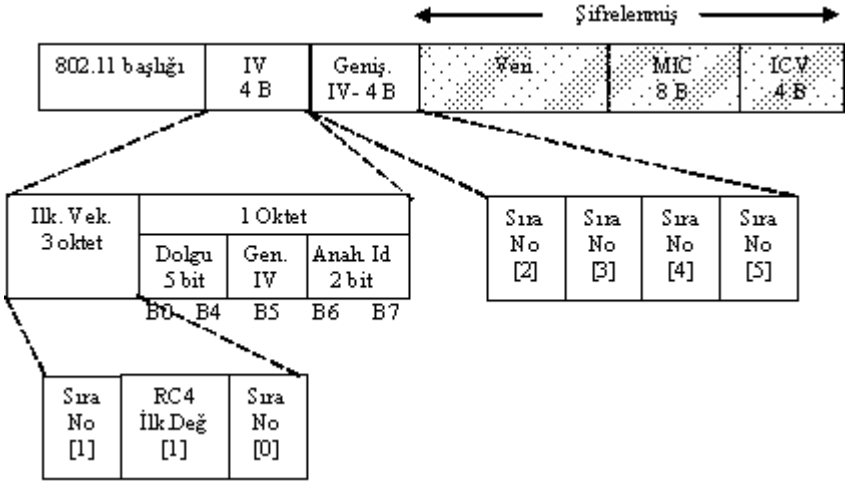
Belirtilen sorunların giderilmesi için TKIP protokolü WEP üzerinde aşağıda verilen değişiklerin yapılamasını öngörür:

- Gönderici mesajı göndermeden önce açık veri, gönderici adres ve alıcı adres üzerinden anahtarlı kriptolojik mesaj bütünlük değeri hesaplar (MIC-Message Integrity Code) ve mesajın sonuna ekler. Eğer gönderme işleminde mesajın bölmelenerek gönderilmesi gerekliyse bütünlük sınaması bölmeleme işleminden önce hesaplanır ve eklenir. Daha sonra her bir parça WEP kapsüllemesi uygulanarak gönderilir. Alıcı kriptolojik bütünlük sınaması değerini, WEP bütünlük sınaması değerini kontrol edip eğer bölmeleme varsa parçaları birleştirdikten sonra yine aynı şekilde hesaplar ve kontrol eder.
- TKIP kriptolojik mesaj bütünlüğü sınaması değeri (TKIP-MIC) tasarım gereklerinden dolayı mesaj değiştirme saldırılarına maruz kalabilecek zayıflık taşır. Mesaj bütünlüğü değerinin bozulmuş olduğunu gören istemci ve erişim noktaları mesaj bütünlüğü saldırıları karşı önlemlerini yürütürler. Böylece saldırganın gerçekleştirebileceği aktif saldırılılar sınırlandırılmış olunur. Karşı önlemler ileriki bölümlerde ele alınacaktır.
- TKIP gönderilen her bir pakette sıra numarası değeri kullanır. Gönderici gönderdiği her pakette sıra numarasını bir arttırır, alıcı tarafta sıralı olarak gelmeyen paketler işlenmez. TKIP sıra numarası değerini IV olarak ve genişletilmiş IV olarak paketin içine kodlar.
- TKIP, RC4 ilklendirme değerinin oluşturulmasında anahtar harmanlama mekanizmasını tanımlar ve kullanır. Bu mekanizma zayıf anahtar saldırılarına karşı bir önlem olarak düşünülmüştür.

5.1.1 Mesaj Formatı

TKIP protokolü WEP kapsülleme mekanizmasında değişiklikler yaparak bu mekanizmayı kullanır. Bölmeleme işleminden önce açık veri, gönderici adres, alıcı adres değerleri üzerinden kriptolojik veri bütünlüğü değeri hesaplanır ve veriye eklenir, toplam 8 sekizlilik bir değerdir. Bölmeleme sonrası her bir parçaya WEP kapsüllemesi uygulanır, öyle ki 48 bitlik sıra numarası değeri paket içerisine IV ve genişletilmiş IV olarak kodlanır. Genişletilmiş IV değeri şifreli veriden hemen önce, IV değerinden sonraya eklenir. Bölmeleme gerekmediği durumda TKIP gönderilecek

WEP paketi üzerinde toplam 12 sekizlilik bir ekleme yapmış olur. Bölmelemenin yapılmadığı durumda paket yapısı Şekil 5-1'de verildiği gibi olacaktır:



Şekil 5-1: TKIP Paketi Yapısı

İlklendirme vektörü anındaki genişletilmiş IV biti (B5) IV alanından sonra genişletilmiş IV alanının varlığını belirtir.TKIP kapsüllemesinde bu bit kurulur ve genişletilmiş IV değeri pakete işlenir. WEP paketleri için bu alan kurulmaz ve genişletilmiş IV pakette yer almaz. Genişletilmiş IV değeri şifrelenmez.

Sıra numarası değeri 48 bitlik bir değerdir ve IV alanı ve genişletilmiş IV alanları kullanılarak iletilir. Sıra numarası aynı zamanda IV değeri olarak da kullanılır. Sıra numarası[0,1] değerleri TKIP anahtar harmanlaması ikinci fazında, sıra numarası[2-5] değerleri anahtar harmanlama aşamasının birinci fazında kullanılır.

İlklendirme vektörü alanında yer alan RC4 ilklendirme değeri[1] sekizlisi sıra numarası olarak kullanılmaz ve değer olarak ((Sıra numarası[1] | (0x20)) & (0x7f)) pakete işlenir.

MIC değeri açık veri, gönderici adres, alıcı adres üzerinden Michael[1] algoritması kullanılarak hesaplanır ve açık verinin sonuna işlenir.

ICV değeri WEP kapsüllemesi tarafından hesaplanan CRC-32 bütünlük sınaması değerini ifade eder.

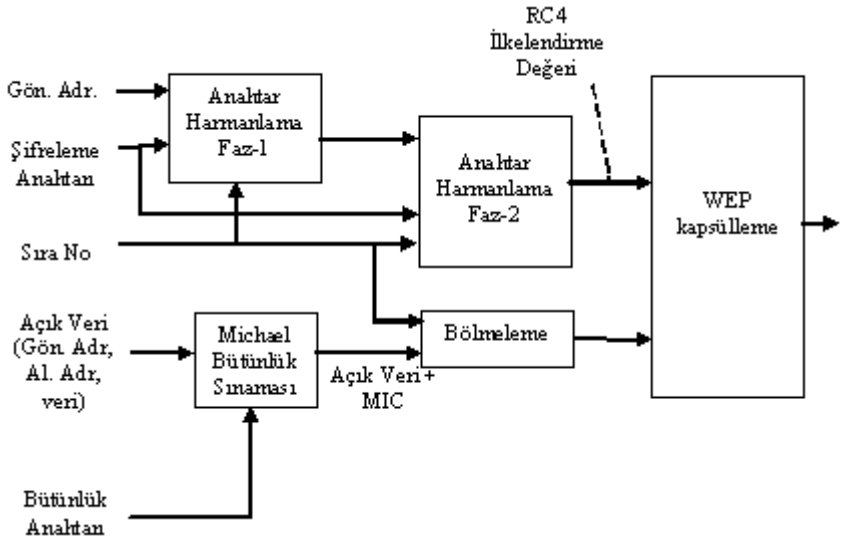
Şifreleme işlemi RC4 algoritması kullanılarak gerçekleştirilir.

[1] Michael anahtarlı kriptolojik veri bütünlüğü algoritmasıdır, ayrıntıları ileriki bölümlerde ele alınacaktır.

5.1.2 Mesaj Gönderim Adımları

1. TKIP MIC değeri gönderici adres, alıcı adres ve açık veri üzerinden Michael algoritması kullanılarak hesaplanır ve açık verinin sonuna işlenir.
2. Eğer gerekliyse mesaj birden fazla paket oluşturacak şekilde bölümlenir. TKIP her bir pakete monoton artan şekilde sıra numarası değeri atar. Sıra numarası değerinin 48 bitlik alanda alabileceği en büyük değere ulaşması sonucu anahtar yenileme işlemi gerçekleştirilmeli veya haberleşme sonlandırılmalıdır. Aksi durum IV yeniden kullanımına yol açmış olur. IV yeniden kullanımının yol açtığı sorunlar WEP protokolü zayıflıklarının anlatıldığı bölümde ele alınmıştır.
3. Her bir paket için TKIP anahtar harmanlama mekanizması kullanılarak RC4 ilklendirme değeri oluşturulur.
4. RC4 ilklendirme değeri ve paket WEP kapsüllemesine gönderilir. Bu aşamada önce WEP ICV değeri CRC-32 kullanılarak hesaplanır ve paketin sonuna eklenir. Daha sonra RC4 ilklendirme değeri ve RC4 algoritması kullanılarak paket şifrelenir.

Mesaj gönderim adımları Şekil 5-2'de gösterilmiştir:

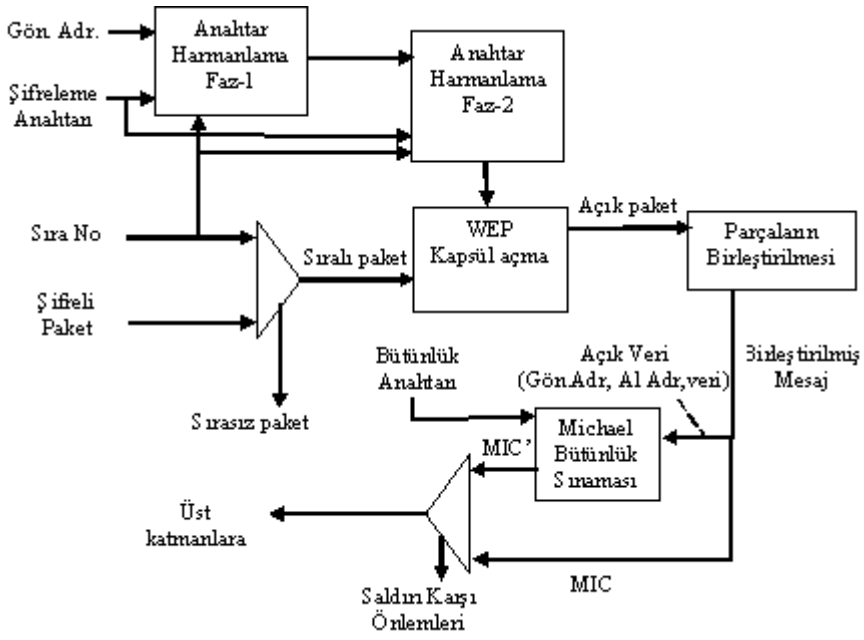


Şekil 5-2: TKIP kapsülleme adımları

5.1.3 Mesaj Alım Adımları

1. Alınan WEP paketi içerisinden IV ve genişletilmiş IV alanından sıra numarası değeri ve anahtar kimlik numarası okunur. Sıra numarası değerine bakılarak sırasız gelen paketler işlenmeden atılır.
2. Sıra numarası ve şifreleme anahtarı kullanılarak RC4 ilklendirme değeri oluşturulur ve paket WEP kapsülü açma işlemleri gerçekleştirilir.
3. WEP ICV sınamasını geçemeyen paketler atılır. Sınamayı geçen paketler bir mesajın farklı parçaları ise birleştirme işlemi uygulanır.
4. Mesaj tek parçadan oluşuyorsa veya birleştirme işlemi tamamlandıysa gönderici adres, alıcı adres ve açık veri üzerinden TKIP MIC değeri Michael algoritması kullanılarak hesaplanır ve mesaj içerisindeki MIC değeri ile karşılaştırılır.
5. Hesaplanan MIC değeri ile mesaj içerisinde gelen MIC değerlerinin farklı olması durumunda veri bütünlüğü saldırıları karşı önlemleri uygulanmaya başlanır. MIC değerleri uyuyorsa paket işlenmek üzere daha üst katmanlara iletilir.,

Mesaj alım adımları Şekil 5-3' de gösterilmiştir:



Şekil 5-3: TKIP kapsül açma adımları

5.2 Mesaj Bütünlüğünün Sağlanması

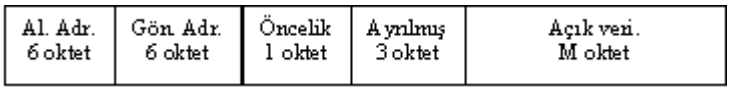
WEP protokolü zayıflıklarından birinin de mesaj bütünlüğünün korunamıyor olması oldu önceki bölümlerde ele alınmıştı. Mesaj bütünlüğünün korunamaması aktif saldırılar için kolaylıklar sağlamaktadır. Veri bütünlüğünün korunamamasının yol açacağı aktif saldırılardan önemlileri şunlardır:

- Bit değiştirme saldırıları
- Mesaja veri ekleme veya veri çıkartma
- Bölmeleme ile ilgili saldırılar
- Gizli anahtara yönelik ötelemeli saldırılar [13, 11]
- Hedef adresinin değiştirilerek paketin farklı adreslere yönlendirilmesi
- Gönderici adresinin değiştirilerek geçerli bir adresten geliyormuş gibi erişim kontrollerini geçmek

TKIP protokolünde veri bütünlüğünün sağlanması için bölmeleme işleminden önce hesaplanan ve açık verinin sonuna eklenen TKIP-MIC tanımlanmıştır.

Kriptolojide TKIP-MIC değerinin hesaplanması için kullanılabilecek, iyi bilinen ve güvenilir bir çok yöntem mevcuttur. Ancak bu yöntemlerin hemen hepsi yoğun işlem gücü gerektiren çarpma gibi matematiksel dönüşümler kullanırlar. Hali hazırda kullanılmakta olan ve işlem kapasiteleri düşük erişim noktaları düşünüldüğünde yüksek işlem gücü gerektiren metotların kullanılması performansı oldukça düşürecektir. Bu nedenle TKIP protokolü için sadece öteleme, yer değiştirme ve ekle işlemlerinin kullanıldığı yalın bir algoritma Niels Ferguson isimli kriptolog tarafından geliştirilmiş ve bu algoritma Michael bütünlük sınaması olarak isimlendirilmiştir. Tasarımındaki kısıtlar ve daha önceden kullanılmış güvenilir bir algoritma olmaması nedeniyle olası veri bütünlüğü saldırıları için TKIP veri bütünlüğü saldırıları karşı önlemlerini tanımlar ve kullanır. Veri bütünlüğü saldırıları karşı önlemleri ileriki bölümlerde ele alınacaktır.

TKIP-MIC toplam 8 sekizli uzunluğunda bir özet değeri üretir. TKIP-MIC hesabında kullanılan Michael algoritmasına giriş olarak alıcı adres, gönderici adres, açık veri ve özet alma işleminde kullanılacak bütünlük anahtarı verilir. Şekil 5-4 kullanılacak girdileri şekil olarak ifade eder:



Şekil 5-4: TKIP-MIC değeri hesabı için girdiler

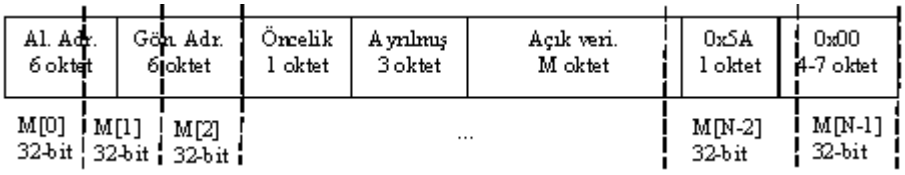
Girdiler yukarıda gösterildiği şekilde ardı ardına eklenerek bir sekizli dizisi oluşturulur. Öncelik alanı 802.11 çerçeve başlığında bulunan ve ileriki kullanımlar için ayrılmış olan öncelik alanıdır. Benzer şekilde ileride kullanabilmek üzere 3 sekizlilik bir ayrılmış alan konulmuştur. Öncelik alanı ve ayrılmış alana sıfır değeri atanır.

Açık veri alanı bölmeleme işleminden önceki gönderilecek tüm mesaj içeriğini kapsar. TKIP-MIC hesaplanması bölmeleme işleminden önce yapılır ve elde edilen özet değeri açık verinin sonuna eklenir. Daha sonra gerekliyse mesaj birden fazla paket oluşturacak şekilde bölmelenebilir. Özet değerinin kontrolü de alıcı tarafta eğer bölmeleme yapıldıysa tüm parçaların gelmesinden ve birleştirme işlemi gerçekleştirildikten sonra yapılır.

5.2.1 Michael Algoritması

TKIP-MIC değerinin hesaplanmasında kullanılan Michael algoritması tasarım kısıtlarından dolayı yalnızca öteleme, yer değiştirme ve ekleme işlemlerini kullanır.

Algoritma uyarınca özet değerinin hesabına başlanılmadan önce; alıcı adres, gönderici adres, öncelik değeri, ayrılmış alan ve açık veriden oluşturulan sekizli dizisinin uzunluğunun 64 bitin katı olmasını garanti etmek için sekizli dizisinin sonuna dolgulama yapılır. Dolgulama işlemi basit yapıdaki erişim noktalarının özet hesabını daha kolay yapabilmeleri için yapılır. Dolgulama alanı veriyle birlikte iletilmez. Dolgulama değerinin ilk sekizlisine (0x5a) değeri atanır. Daha sonra sekizli dizisinin boyuna göre 4 ila 7 sekizlilik 0x00 değeri eklenir. Dolgulanmış sekizli dizisi 32 bitlik bloklara ayrılır. Şekil 5-5 anlatılanları şekil olarak ifade eder:



Şekil 5-5: Dolgulama yapılmış Michael algoritması bilgi girişi

32 bitlik bloklara ayrılmış, dolgulanmış sekizli dizisinin i. bloğunu M[i-1] ile gösterelim. Bu durumda 32 bitlik N bloğa ayrılmış dolgulanmış sekizli dizisinin sonuncu bloğu M[N-1] = 0 ve M[N-2] ≠ 0 olacaktır.

Michael algoritmasında kullanılan bütünlük anahtarı 64 bitlik (8 sekizli) bir anahtardır ve şifreleme işleminin yapılacağı anahtardan farklı olmalıdır. 64 bitlik bu anahtarı 32 bitlik iki blok halinde K = (K[0] || K[1]) olarak gösterelim.

Michael algoritması aşağıda verildiği şekilde tanımlanmıştır:

Michael((K[0] || K[1]), (M[0] || M[1].....M[N-1]))

(L, R) ← (K[0], K[1])

for i =0 to N-1 do

L ← L ⊕ M[i]

(L, R) ← funcMic(L, R)

End

MIC = L || R

End

Algoritmada kullanılan funcMic() fonksiyonu da aşağıda verilmiştir:

funcMic(L, R)

R ← R ⊕ (L << 17)

L ← (L + R) mod 2^{32}

R ← R ⊕ XSwap(L)

L ← (L + R) mod 2^{32}

R ← R ⊕ (L << 3)

L ← (L + R) mod 2^{32}

R ← R ⊕ (L >> 2)

L ← (L + R) mod 2^{32}

return (L, R)

End

Xswap(i) fonksiyonu 32 bitlik bir sayının ilk 16 biti ile son 16 bitinin yerini değiştirir. Örneğin Xswap(12345678) = 56781234 olacaktır.

>> işareti sayının sağa öteleneceğini gösterir.

<< işareti sayının sola öteleneceğini gösterir.

5.2.2 Mesaj Bütünlüğü Saldırıları Karşı Önlemleri

Tasarımındaki kısıtlar ve daha önceden kullanılmış güvenilir bir algoritma olmaması nedeniyle olası veri bütünlüğü saldırıları için TKIP, veri bütünlüğü saldırıları karşı önlemlerini kullanır. TKIP-MIC değeri kontrol edilmeden önce alıcı aldığı tüm paketler için sıra numarası kontrolü, çerçeve çevrimli fazlalık sınaması kontrolü ve WEP-ICV kontrolü adımlarını yürütür. Çerçeve çevrimli fazlalık sınaması ve WEP-ICV kontrolleri ortamdaki gürültüden oluşabilecek hataları anlayabilmek için yeterli olacaktır. Mesaj bütünlük sınaması hatası (TKIP-MIC) olası bir aktif saldırının gerçekleştiriliyor olduğunu gösterir. TKIP veri bütünlüğü saldırıları karşı önlemlerinin amacı aşağıda verildiği gibi sıralanabilir:

- TKIP-MIC hatası güvenlik ihlali ile ilgili bir alarm üretmeli ve bu alarm kayıt edilmelidir.
- Olası TKIP-MIC hataları dakikada ikiden fazla olmamalıdır. Yani aynı dakika içerisinde birden fazla TKIP-MIC hatası ile karşılaşan istemci ve/veya erişim noktası haberleşmeye devam etmek için 60 saniye beklemelidir. Böylelikle saldırgan için ardı ardına gerçekleştirebileceği aktif saldırı miktarı kısıtlanmış olunur.
- Gerek görüldüğü takdirde mevcut anahtarlar güncellenmelidir.

İstemcilerin TKIP-MIC hatası fark etmesi durumunda bu hatayı erişim noktasına bildirmeleri gereklidir. Bu amaçla EAPOL-Anahtar paketleri kullanılır. TKIP-MIC hatasını bildiren EAPOL-Anahtar paketinde özet, hata, istek ve güvenli bayrakları kurulur ve istemci mevcut karşılıklı haberleşme anahtarlarını kullanarak göndereceği mesajın özetini hesaplayarak paketin içerisine yerleştirir.

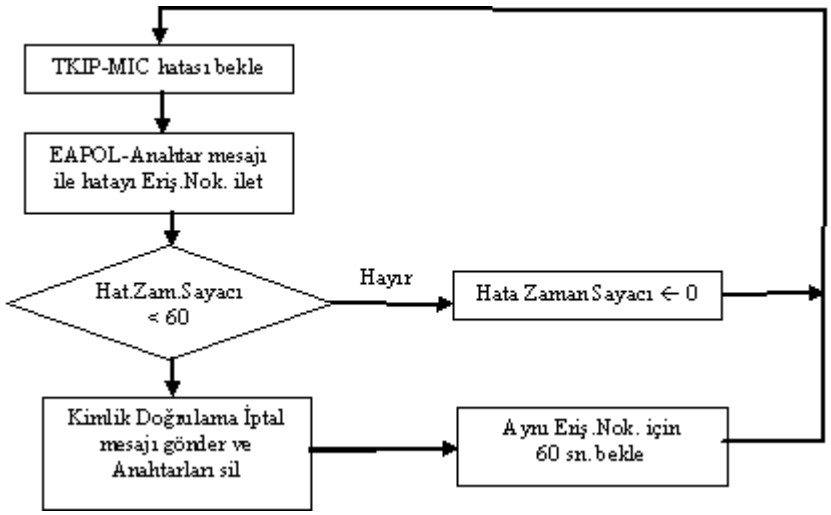
Erişim noktası aynı dakika içerisinde birden fazla TKIP-MIC hatası ile karşılaşırsa veya TKIP-MIC hatası bildiren EAPOL-Anahtar paketi alırsa kendisine bağlı tüm istemcileri siler ve yeniden haberleşmeye başlamak için 60 saniye bekler.

5.2.2.1 İstemcilerin Uygulayacağı Adımlar

Kendisine gelen mesajda TKIP-MIC bütünlük sınaması değerinin yanlış olduğunu fark eden istemci aktif bir saldırı ile karşı karşıya kaldığını düşünerek aşağıda belirtilen adımları yürütür:

1. TKIP-MIC hatası sayacını bir arttır.
2. TKIP-MIC hatası fark edilen mesajı işlemeden at.
3. Erişim noktasına TKIP-MIC hatasını belirten EAPOL-Anahtar mesajı gönder.
4. Hata zaman sayacı 60 saniyeden büyükse yani son bir dakika içerisinde karşılaşılan ilk TKIP-MIC hatası ise hata zamanı sayacını sıfırla.
5. Hata zaman sayacı 60 saniyeden küçükse, yani son bir dakika içerisinde karşılaşılan ikinci TKIP-MIC hatasıysa erişim noktasına kimlik doğrulama iptalinin TKIP-MIC hatası sebebiyle gerçekleştirildiğini belirten kimlik doğrulama iptali mesajı gönder ve mevcut karşılıklı haberleşme ve grup anahtarlarını sil.
6. Aynı erişim noktası ile TKIP protokolünün kullanılacağı haberleşme birliğini tekrar kurmak için 60 saniye bekle veya bir başka erişim noktası ile haberleşme birliği kur.

Şekil 5-6, istemciler için TKIP-MIC hatası karşı önlemlerini şekil olarak gösterir:



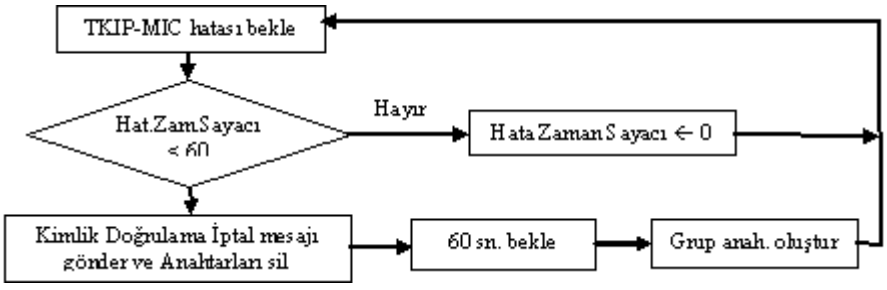
Şekil 5-6: İstemci için TKIP-MIC hatası karşı önlemleri

5.2.2.2 Erişim Noktalarının Uygulayacağı Adımlar

Kendisine gelen mesajda TKIP-MIC bütünlük sınaması değerinin yanlış olduğunu fark eden veya istemcilerden TKIP-MIC hatasını belirten EAPOL-Anahtar mesajı alan erişim noktası aktif bir saldırı ile karşı karşıya kaldığını düşünerek aşağıda belirtilen adımları yürütür:

1. Hatanın oluştuğu yere göre
    a. Kendisine gelen bir mesajda TKIP-MIC hatası varsa yerel TKIP-MIC hatası sayacını bir arttır ve ilgili mesajı işlemeden at.
    b. İstemcilerden TKIP-MIC hatasını belirten EAPOL-Anahtar mesajı alındıysa uçbirim TKIP-MIC hatası sayacını bir arttır.
2. Hata zaman sayacı 60 saniyeden büyükse yani son bir dakika içerisinde karşılaşılan ilk TKIP-MIC hatası ise hata zamanı sayacını sıfırla.
3. Hata zaman sayacı 60 saniyeden küçükse, yani son bir dakika içerisinde karşılaşılan ikinci TKIP-MIC hatasıysa kimlik doğrulama iptalinin TKIP-MIC hatası sebebiyle gerçekleştirildiğini belirten kimlik doğrulama iptali mesajını tüm istemcilere gönder ve mevcut karşılıklı haberleşme ve grup anahtarlarını sil.
4. Karşılıklı kimlik doğrulama için 802.1X kullanılıyorsa asıllayıcı anahtar durum makinesini İlklendir durumuna geçir.
5. TKIP protokolünün kullanılacağı haberleşme birliklerini tekrar kurmak için 60 saniye bekle.
6. 60 saniye sonunda grup anahtarını yeniden oluştur ve haberleşme birliklerini yeniden kurmaya başla.

Şekil 5-7, erişim noktaları için TKIP-MIC hatası karşı önlemlerini şeklen gösterir:

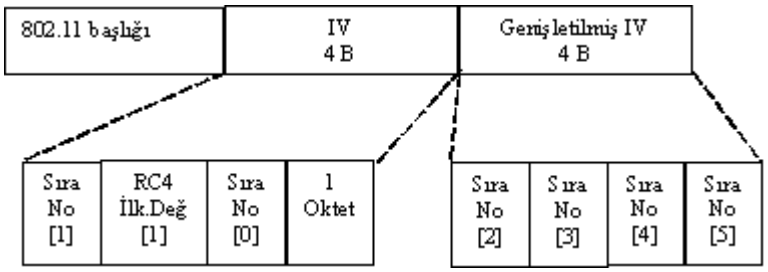


Şekil 5-7: Erişim noktası için TKIP-MIC hatası karşı önlemleri

5.3 Sıra Numarası ve Kullanımı

WEP protokolünün paket tekrarı saldırılarına karşı koymak için herhangi bir mekanizma kullanmadığı ve paket tekrarı saldırılarına açık olduğu geçen bölümlerde ele alınmıştır. Paket tekrarı saldırılarında saldırgan paketin şifresini çözmek için çaba sarf etmez, onun yerine şifreli paketlerle yapılan işlemi tahmin etmeye çalışır ve yakaladığı şifreli ve geçerli paketleri tekrar göndererek saldırıyı gerçekleştirir. Örneğin WEP kapsüllemesi yapılmış şifreli paketlerin hesaplar arası para transferinin yapıldığı bir bankacılık işlemine ait verileri taşıdığını düşünürsek, saldırgan yakaladığı mesajları tekrar göndererek hesaplar arası aktarılan para miktarını değiştirebilir.

Tekrar saldırılarının engellenmesi amacıyla TKIP protokolü için sıra numarası tanımlanmıştır. Sıra numarası 48 bitlik (6 sekizli) bir sayıdır ve 802.11 paketi içerisinde IV ve genişletilmiş IV alanlarında taşınır. Her paket için farklı olması gereken sıra numarası değeri aynı zamanda şifreleme ve şifre çözme işlemlerinde IV değeri olarak ta kullanılır. Zaten her paket için farklı olması gereken sıra numarası IV olarak kullanılacağından IV tekrar kullanımı problemi de oluşmamış olacaktır. Ayrıca sıra numarası[0] ve sıra numarası[1] sekizlileri TKIP anahtar harmanlaması ikinci fazında, sıra numarası[2-5] değerleri de anahtar harmanlama aşamasının birinci fazında kullanılır. Şekil 5-8, sıra numarası değerinin 802.11 çerçevesine kodlanmasını gösterir.



Şekil 5-8: TKIP sıra numarası değerinin 802.11 çerçevesine kodlanması

Sıra numarası kullanılarak paket tekrarı saldırılarının önlenmesi için 802.11i standardında belirtilen adımlar aşağıda verilmiştir:

- Her pakette farklı olacak şekilde TKIP sıra numarası verilir.

- Her gönderici kendisinde mevcut her karşılıklı haberleşme anahtarı ve grup anahtarı için ayrı birer sıra numarası değeri tutarlar.
- Sıra numarası ilgili anahtar oluşturulduğunda veya yenilendiğinde sıfırlanan 48 bitlik monoton artan bir sayıdır.
- Sıra numarasının düşük anlamlı 16 biti WEP IV alanında taşınır ve TKIP anahtar harmanlama mekanizmasının ikinci fazında da kullanılır. Sıra numarasının geri kalanı 802.11 çerçevesinde genişletilmiş IV alanında taşınır ve TKIP anahtar harmanlama mekanizmasının birinci fazında kullanır.
- Her alıcı karşılıklı haberleşme ve grup anahtarları için ayrı bir yerel sıra numarası değeri tutar.
- Alıcılar sıra numarası değerini paketi ilk aldıklarında kontrol ederler fakat tuttukları yerel sıra numarası değerini arttırmak için TKIP-MIC kontrolünün başarıyla tamamlanmasını beklerler.
- Alınan paket içerisinden okunan sıra numarası değerinin alıcı tarafta tutulan yerel sıra numarası değerinden küçük veya yerel sıra numarası değerine eşit olması paketin tekrar edilen bir paket olduğunu gösterir.
- Sıra numarası kontrolünden geçemeyen paketler işlenilmeden atılır ve ilgili sayaç bir arttırılarak paket tekrarı kayıt altına alınır.

5.4 Anahtar Harmanlama Mekanizması

TKIP anahtar harmanlama mekanizması şifrelenecek her pakette farklı bir anahtar kullanmak için düşünülmüştür. Her paket için farklı anahtar kullanılmak istenmesi RC4 zayıf anahtar saldırılarına karşı koymak ve genişletilmiş IV değerinin şifreleme işlemine dahil edilmesini sağlamak içindir.

Yapılan işlem, oturum anahtarı (geçici karşılıklı haberleşme anahtarı), IV (sıra numarası) ve gönderici adresi değerlerini özel bir özet alma fonksiyonundan geçirerek RC4 ilklendirme değerinin oluşturulmasıdır.

Özet alma işlemleri genellikle yüksek işlem gücü gerektireceğinden ve gönderilecek her paket için özet alma fonksiyonu kullanılarak paket anahtarı oluşturacağından özellikle düşük işlem güçlü erişim noktalarında performans düşüklüğüne yol açacaktır. Bu nedenle anahtar harmanlama mekanizması iki aşamalı olacak şekilde

bölünmüştür. İlk aşamaya oturum anahtarı, gönderici adresi ve sıra numarasının yüksek anlamlı 4 sekizlisi katılarak ilk aşama sonrası elde edilecek değerin 65.535 paket için değişmeden kullanılabilir olması sağlanmıştır. İkinci aşamada oturum anahtarı, sıra numarasının düşük anlamlı 2 sekizlisi ve ilk aşamada oluşturulan değer girdi olarak kullanılır. İkinci aşama gönderilecek her pakette tekrarlanarak RC4 ilklendirme değeri oluşturulur:

TTAK[1] =Faz1(Oturum Anahtarı, Gönderici Adres, Sıra No[2-5])

RC4 ilklendirme değeri = Faz2(TTAK, Oturum Anahtarı, Sıra No[0,1])

TKIP anahtar harmanlama mekanizmasında, 802.11i standardında tanımlı olan 256*2 sekizlilik bir değiştirme kutusu (SBox) kullanılır. Değiştirme kutusu değerleri TKIP kullanmak isteyen tüm gerçeklemelerde aynı olmalıdır.

5.4.1 TKIP Anahtar Harmanlama Mekanizması Birinci Fazı

TKIP anahtar harmanlama birinci fazında oturum anahtarı, gönderici adresi ve sıra numarasının yüksek anlamlı 4 sekizlisi kullanılır ve 80 bitlik TTAK değeri üretilir. Anahtar harmanlama birinci fazı hesaplandıktan sonra gönderilecek 65.535 paket için değişmez. TKIP anahtar harmanlama mekanizması birinci fazı aşağıda verildiği gibidir:

TKIP Anahtar Harmanlama Faz1(Gönderici Adres[0-5], Oturum Anahtarı[0-15], Sıra No[2-5])

TTAK[0] ← Mk16(Sıra No[3], Sıra No[2])

TTAK[1] ← Mk16(Sıra No[5], Sıra No[4])

TTAK[2] ← Mk16(Gön.Adr.[1], Gön.Adr.[0])

TTAK[3] ← Mk16(Gön.Adr.[3], Gön.Adr.[2])

TTAK[4] ← Mk16(Gön.Adr.[5], Gön.Adr.[4])

for i = 0 to LOOP_COUNT-1 //LOOP_COUNT = 8

j ← 2*(i&1)

[1]TTAK: Anahtar harmanlama mekanizması birinci fazı sonucunda oluşturulan 80 bitlik değer.(TKIP mixed Transmit Address and Key)

TTAK[0] ← TTAK[0] + Sbox[TTAK[4] ⊕ Mk16(Ot.An.[1] + j, Ot.An[0] +j)]

TTAK[1] ← TTAK[1] + Sbox[TTAK[0] ⊕ Mk16(Ot.An.[5] + j, Ot.An[4] +j)]

TTAK[2] ← TTAK[2] + Sbox[TTAK[1] ⊕ Mk16(Ot.An.[9] + j, Ot.An[8] +j)]

TTAK[3] ← TTAK[3] + Sbox[TTAK[2] ⊕ Mk16(Ot.An.[13] + j, Ot.An[12] +j)]

TTAK[4] ← TTAK[4] + Sbox[TTAK[3] ⊕ Mk16(Ot.An.[1] + j, Ot.An[0] +j)] + i

End

End

Mk(X, Y) işlemi 8 bitlik X ve Y sayılarını kullanarak 16 bitlik (256*X) + Y işlemini ifade eder.

TTAK değeri 16 bitlik bloklar halinde ve TTAK[i] şeklinde gösterilmiştir.

5.4.2 TKIP Anahtar Harmanlama Mekanizması İkinci Fazı

TKIP anahtar harmanlama ikinci fazında oturum anahtarı, sıra numarasının düşük anlamlı 2 sekizlisi ve birinci fazda üretilen 80 bitlik TTAK değeri kullanılır, sonuç olarak 128 bitlik RC4 ilklendirme değeri oluşturulur. TKIP anahtar harmanlama ikinci fazı gönderilecek her paket için tekrar yürütülür. TKIP anahtar harmanlama mekanizması ikinci fazı aşağıda verildiği gibidir:

TKIP Anahtar Harmanlama Faz2(TTAK[0-4], Oturum Anahtarı[0-15], Sıra No[0,1])

PPK[0] ← TTAK[0]

PPK[1] ← TTAK[1]

PPK[2] ← TTAK[2]

PPK[3] ← TTAK[3]

PPK[4] ← TTAK[4]

PPK[5] ← TTAK[4] + Mk16(Sıra No[1], Sıra No[0])

PPK[0] ← PPK[0] + Sbox[PPK[5] ⊕ Mk16(Ot.An.[1], Ot.An.[0])]

PPK[1] ← PPK[1] + Sbox[PPK[0] ⊕ Mk16(Ot.An.[3], Ot.An.[2])]

PPK[2] ← PPK[2] + Sbox[PPK[1] ⊕ Mk16(Ot.An.[5], Ot.An.[4])]

PPK[3] ← PPK[3] + Sbox[PPK[2] ⊕ Mk16(Ot.An.[7], Ot.An.[6])]

PPK[4] ← PPK[4] + Sbox[PPK[3] ⊕ Mk16(Ot.An.[9], Ot.An.[8])]

PPK[5] ← PPK[5] + Sbox[PPK[4] ⊕ Mk16(Ot.An.[11], Ot.An.[10])]

PPK[0] ← PPK[0] + Rot(PPK[5] ⊕ Mk16(Ot.An.[13], Ot.An[12])

PPK[1] ← PPK[1] + Rot(PPK[0] ⊕ Mk16(Ot.An.[15], Ot.An[14])

PPK[2] ← PPK[2] + Rot(PPK[1])

PPK[3] ← PPK[3] + Rot(PPK[2])

PPK[4] ← PPK[4] + Rot(PPK[3])

PPK[5] ← PPK[5] + Rot(PPK[4])

RC4 İlk.Değ.[0] ← Sıra No[1]

RC4 İlk.Değ.[1] ← (Sıra No[1] | 0x20) & 0x7f

RC4 İlk.Değ.[2] ← Sıra No[0]

RC4 İlk.Değ.[3] ← Lo8((PPK[5] ⊕ Mk16(Ot.An.[1], Ot.An[0])) >> 1)

for i = 0 to 5

RC4 İlk.Değ.[4 +(2*i)] = Lo8(PPK[i])

RC4 İlk.Değ.[5 +(2*i)] = Hi8(PPK[i])

End

Return RC4 İlk.Değ.[0-15]

End

PPK[i] ikinci faz işlemlerinde kullanılan 16 bitlik geçici sayıyı ifade eder.

Rot(X) işlemi 16 bitlik X sayısının sağa 1 bit öteleneceğini ifade eder.

Lo8(X) işlemi 16 bitlik X sayısının düşük anlamlı 8 bitinin alınacağını ifade eder.

Hi8(X) işlemi 16 bitlik X sayısının yüksek anlamlı 8 bitinin alınacağını ifade eder.

6 CCMP

CCMP (Counter Mode-CBC MAC Protocol, Sayaçlı-Blok Zincirleme Mesaj Bütünlüğü Protokolü) 802.11i standardı için gerçekleştirilmesi zorunlu güvenlik mekanizmasını tanımlar. CCMP veri gizliliğini, veri kaynağının doğrulanmasını, veri bütünlüğünü ve tekrar korumasını sağlar, AES (Advanced Encryption Standart, Gelişmiş Şifreleme Standardı) şifreleme algoritmasını kullanır.

CCMP protokolü TKIP' in aksine bir geçiş protokolü değil 802.11 ağları için nihai güvenlik mekanizmalarını tanımlar ve önceden yapılmış güvenlik amaçlı uygulamaları (WEP kapsülleme) geçersiz kılarak kullanmaz. CCMP protokolü TKIP' e oranla daha güvenilir kabul edilmektedir. Bunun nedeni eskiye olan bağımlılığının olmaması ve telsiz bilgisayar ağları üzerinde koşturulacağı da göz önüne alınarak baştan tasarlanmış olmasıdır.

Şifreleme algoritması kurulacak güvenlik mekanizmasının kalbi olarak tanımlanacağından bilinen problemlerinden dolayı RC4 algoritması yerine daha güvenilir bir algoritma olan AES seçilmiştir. RC4 algoritması temelde şifreleme amaçlı olarak değil rasgele sayı üretme amaçlı tasarlanmış olması da algoritma değişiminin bir nedenidir.

Sadece şifreleme algoritmasını değiştirmek zayıf bir protokol tasarlandığında etkili bir çözüm olmayacaktır. Yine WEP örneği ele alınırsa protokol yapısındaki problemlerden dolayı gerçekte rasgeleye yakın sayılar üretebilen RC4 algoritması yanlış kullanımı sonucu güvensiz olarak damgalanmıştır. Bu nedenle uygulanacak kapsülleme mekanizması en az algoritma kadar önem taşıyacaktır.

6.1 AES

AES algoritması blok şifreleme algoritmasıdır. Matematiksel ve lojik işlemler kullanılarak anahtar ve belli uzunluktaki açık veriyi alır yine aynı uzunlukta şifreli veriye çevirecek dönüşümler tanımlar. AES algoritması tersinir bir algoritmadır.

Yani aynı anahtar kullanılarak şifrelenmiş veri çözülerek açık veri elde edilebilir. Anahtarı bilmeden açık veriyi elde etmek imkansızdır.

AES algoritması Joan Daeman ve Vincent Rijmen tarafından gerçekleştirilmiş Rijndael algoritmasını temel alır. Rijndael algoritması Amerika Birleşik Devletleri Ulusal Bilim ve Teknoloji Enstitüsü (NIST) tarafından 2000 senesinde açılan şifreleme algoritması yarışmasına katılarak kazanmış ve üzerinde bir takım değişiklikler yapılarak ABD için şifreleme standardı olarak kabul edilmiş [23] ve AES adını almıştır.

Rijndael algoritması blok boyu ve anahtar boyu olarak 128 bit, 192 bit veya 256 biti ayrı ayrı kullanabilir. Yani anahtar boyu 128 bitken blok boyu 256 bit olabilir. NIST Rijndael algoritmasını AES olarak kabul ederken blok boyu olarak 128 biti sabit almıştır. AES için anahtar boyu yine üç değerden biri olabilir. 802.11i kullanacağı AES algoritması için blok boyunun yanı sıra anahtar boyunu da 128 bit olacak şekilde sabitlemiştir.

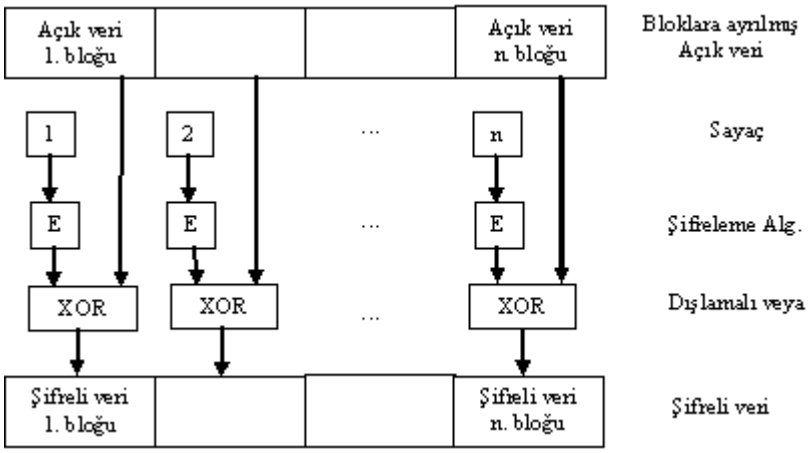
AES algoritması 128 bitlik bir bloğu şifreleyecek şekilde tanımlanmıştır. Değişken uzunluklu verinin 128 bitlik bloklara ayrılması ve bu blokların algoritma uyarınca şifrelenmesi, şifreli blokların uygun bir sırada yan yana getirilerek şifreli verinin oluşturulması ve alıcı tarafta tersine işlemler uygulanarak şifrenin çözülerek açık verinin elde edilmesi işlemlerine algoritmanın çalıştırılma modu denilir. NIST tarafından AES şifreleme algoritması kullanan değişik çalıştırılma modları tanımlanmıştır [24]. 802.11i standardı CCM[24, 25] olarak adlandırılan çalıştırma modunu ve AES blok şifreleme algoritmasını kullanır.

6.1.1 CCM Modu

Şifreleme algoritmaları farklı modlarda koşturularak farklı amaçlar için özelleştirilebilirler. Örneğin NIST, AES algoritması için tanımlanacak çalıştırma modlarını halen incelemekte ve kabul ettiklerini Web sayfasında duyurmaktadır [24].

CCM (Counter Mode-CBC MAC) çalıştırma modu özellikle telsiz bilgisayar ağlarında kullanılmak üzere 802.11i çalışma grubunda yer alan kriptolog Doug Whiting, Russ Housley ve Niels Ferguson tarafından geliştirilmiştir. CCM modu aynı zamanda IPSec [26] tarafından kullanılması önerisiyle IETF (Internet Engineering Task Force)' e iletilmiştir [25].

CCM modu iki farklı çalıştırma modu olan sayaçlı çalıştırma modu (Counter mode) ve blok zincirleme modlarının (CBC mode) birlikte kullanılmasını gerektirir. Sayaçlı şifreleme modu kriptoloji dünyasında yıllardır kullanılan ve güvenilen bir çalıştırma modudur. Bu modda veri bloklara ayrıldıktan sonra her bir blok şifrelenmiş sayaç numarası ile dışlamalı veya işleminden geçirilerek şifreli veri elde edilir. Şekil 6-1' de sayaçlı şifreleme modu verilmiştir:



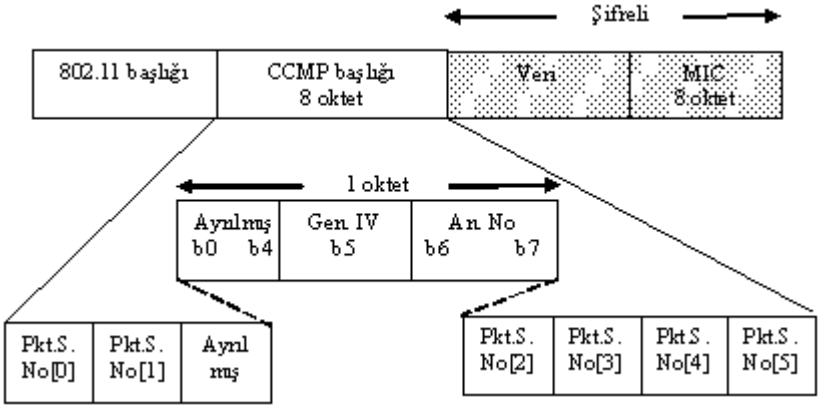
Şekil 6-1: Sayaçlı şifreleme modu

Sayaçlı çalışma modu çıktı olarak yalnızca şifrelenmiş veri üretir. Ayrıca bütünlük sınaması ve kaynak doğrulamada kullanılacak bir mekanizmaya gerek duyulmaktadır. Bu amaçla da yine kriptoloji dünyasında sıkça kullanılan blok şifreleme algoritmalarının bir çalıştırma modu olan blok zincirleme mesaj bütünlüğü (CBC-MAC) kullanılmıştır. CBC-MAC çalıştırma modunda ilk açık veri bloğu şifreleme algoritması (AES) uyarınca şifrelenir, sonuçta elde edilen şifreli blok ikinci açık veri bloğu ile dışlamalı veya işleminden geçirilir ve elde edilen sonuç tekrar şifrelenir. Bu şekilde son bloğa kadar işlem devam ettirilir. Son açık veri bloğuna da aynı işlem uygulandıktan sonra elde edilen şifreli blok tüm mesajın bütünlük sınaması değeri olarak kullanılır.

Her iki modun da tek anahtarla çalıştırılmasının güvenlik açığı yaratmayacağı öne sürülmektedir [27] ve 802.11i standardında önerildiği şekilde her iki çalıştırma modu da tek anahtarla yürütülmektedir.

6.2 CCMP Mesaj Formatı

CCMP kapsülleme 802.11-1999 standardında yer alan WEP kapsülleme işleminin yerine tanımlanmıştır. CCMP kapsülleme işlemi mesaj eğer gerekli ise bölmeleme işlemi yapıldıktan sonra her bir parçaya ayrı ayrı uygulanır. CCMP kapsülleme işlemi paket boyunu 8 sekizli CCMP başlığı ve 8 sekizli veri bütünlüğü sınaması değeri olmak üzere 16 sekizli arttırır. Bölmeleme işlemi yapılacaksa CCMP' nin paket boyunu 16 sekizli artıracağı göz önünde bulundurulmalıdır. CCMP kapsülleme işlemi uygulandıktan sonra paket yapısı Şekil 6-2' de verildiği gibi olacaktır:

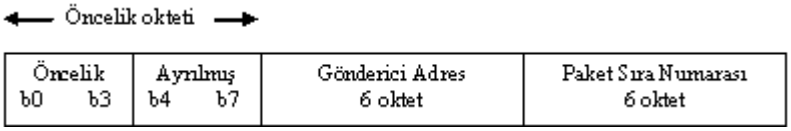


Şekil 6-2: CCMP paket formatı

Genişletilmiş IV bayrağı CCMP protokolü kullanılacaksa her zaman kurulur. Paket sıra numarası değeri 48 bitlik bir değerdir ve IV ve genişletilmiş IV alanlarında taşınır. Ayrılmış alanlara gönderici tarafından sıfır yazılmalıdır. CCMP başlığı şifresiz açık olarak gönderilir. CCMP-MIC değeri açık veri ve 802.11 başlığı ve CCMP başlığı üzerinden CBC-MAC algoritması kullanılarak hesaplanır ve paket içerisine yazılarak şifrelenir. AES CBC-MAC 128 bitlik bir çıktı üretir, bu çıktının ilk 64 biti (8 sekizli) MIC değeri olarak kullanılır.

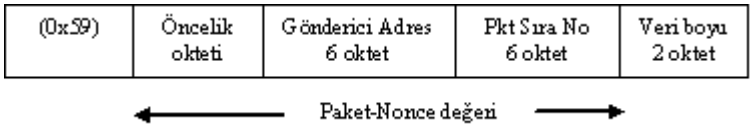
6.3 CCMP Mesaj Gönderim Adımları

1. Paket sıra numarasını bir arttır ve pakete işle. Aynı sıra numarası değeri aynı anahtar için paket tekrar gönderimi haricinde tekrar kullanılamaz.
2. Paket önceliği değeri, gönderici adres ve paket sıra numarasını kullanarak 13 sekizlilik paket-Nonce değerini oluştur. CCMP paket-Nonce değeri Şekil 6-3' de şekil olarak gösterilmiştir:



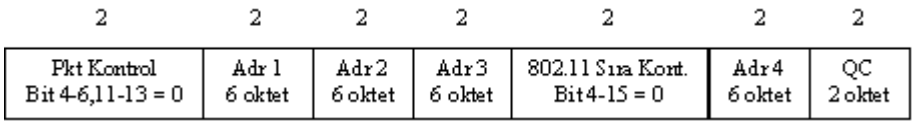
Şekil 6-3: CCMP paket-Nonce değerinin oluşturulması

3. Oluşturulan paket-Nonce değeri, paket içerisinde taşınan veri boyunu ve sabit (0x59) değerini kullanarak CBC-MAC algoritmasına verilecek ilk bloğu oluştur. CCMP CBC-MAC ilk bloğu Şekil 6-4' de şekil olarak gösterilmiştir:



Şekil 6-4: CBC-MAC ilk bloğunun oluşturulması

4. 802.11 başlığındaki değerleri kullanarak Ek Bütünlük-Kimlik Doğrulama Değeri (AAD-Additional Authentication Data) oluştur. 802.11 başlığında değişebilecek alanlara sıfır yaz. CCMP-AAD değeri Şekil 6-5' de şekil olarak gösterilmiştir:

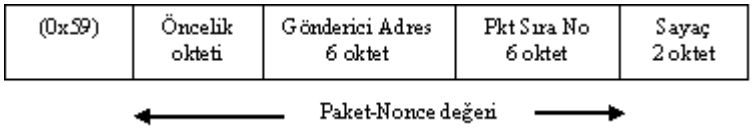


Şekil 6-5: CCMP-AAD değerinin oluşturulması

(Adres 4 ve servis kalitesini belirten QC (Quality of Service Control) alanı bulunmaya bilir.)

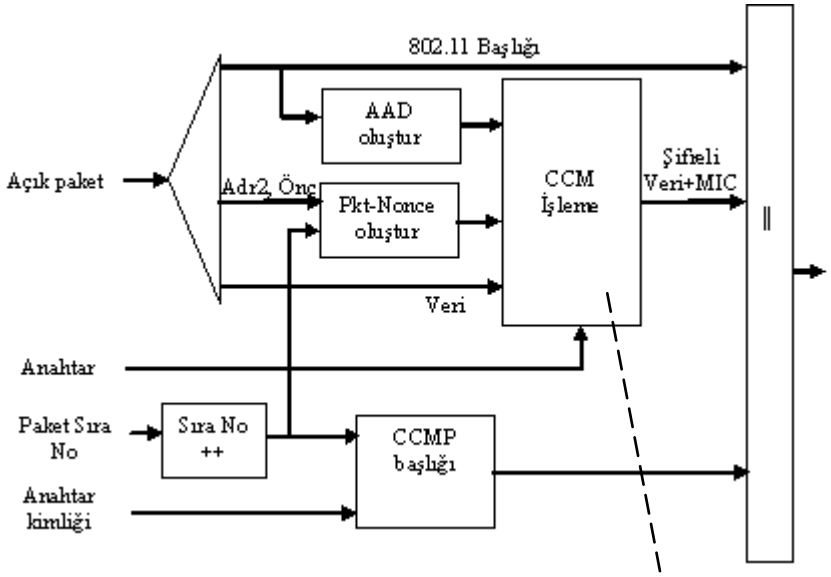
5. AES CBC-MAC algoritmasını ve şifreleme anahtarını kullanarak 3.adımda oluşturulan CBC-MAC ilk bloğundan başla, daha sonra AAD değerine geç ve en son olarak açık veri CBC-MAC uyarınca işle. Sonuç olarak 128 bitlik bir bütünlük sınaması değeri elde edilir. Bu değerin yüksek anlamlı ilk 64 bitini (8 sekizli) alınarak açık verinin sonuna ekle.
6. Şifrelenecek açık veri ve açık verinin sonuna eklenen özet değerini 128 bitlik bloklara ayır. Şifreleme işleminde kullanmak üzere paket-Nonce değerini, sabit (0x59) değerini kullanarak sayaç değerini oluştur. Sayaç değerini

işlenilen her blokta bir arttır. AES algoritmasını sayaçlı çalışma modunda koştur ve sayaç olarak oluşturulan sayaç değerini kullan. CCMP şifrelemesinde kullanılacak sayaç değerinin oluşturulması Şekil 6-6' da şekil olarak gösterilmiştir:

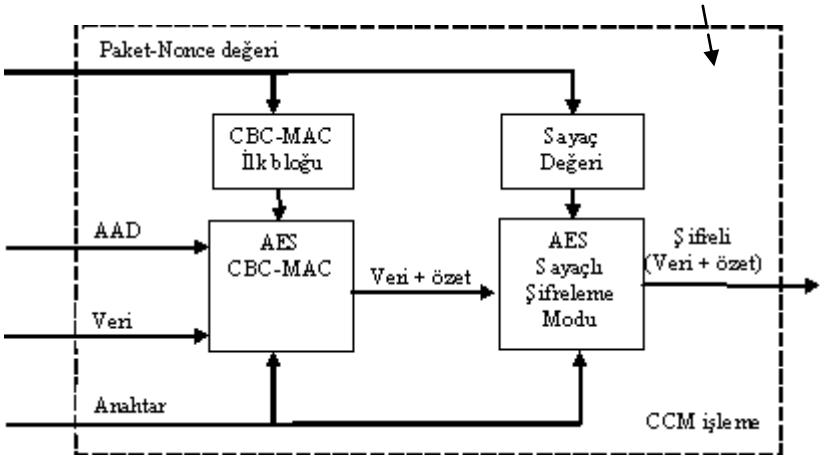


Şekil 6-6: CCMP şifrelemesinde kullanılacak sayaç değerinin oluşturulması

CCMP mesaj gönderim adımları Şekil 6-7 ve Şekil 6-8' de şekil olarak özetlenmiştir:



Şekil 6-7: CCMP paket gönderim adımları



Şekil 6-8: CCM işleme adımları gösterimi

6.4 CCMP Mesaj Alım Adımları

CCMP uygulanarak gönderilen paket alıcı tarafta benzer işlemlerden geçirilir ve gerekli kontrollerden geçtiyse işlenmek üzere üst katmanlara iletilir. CCMP mesaj alım adımları verildiği gibidir:

1. CCMP başlığında yer alan paket sıra numarası değerini yerel sıra numarasıyla karşılaştır. Gelen paketteki sıra numarası değeri yerel sıra numarası değerine eşitse veya ondan küçükse paketi işlemeden at.
2. Gelen paket teke-gönderim ise karşılıklı haberleşme anahtarını, çoğa-gönderim ise grup anahtarını bul.
3. Gelen paket içerisinden sıra numarası ve gönderici adresi oku ve paket-Nonce değerini oluştur. Paket-Nonce değerini kullanarak sayaç değerini oluştur.
4. Gizli anahtar ve sayaç değerini kullanarak AES algoritmasını sayaçlı çalıştırma modunda yürüterek gelen verinin şifresini çöz.
5. 802.11 başlığını kullanarak AAD değerini oluştur. AAD ve şifresi çözülen verinin özetini AES algoritmasını CBC-MAC modunda yürüterek ve gizli anahtarı da kullanarak tekrar hesapla.
6. Hesaplanan özet değeri ile paket içerisinde yer alan özet değerini karşılaştır. İki değer birbirinden farklıysa paketi at.
7. Hesaplanan özet değeri ile paket içerisinde yer alan özet değeri aynıysa yerel sayaç numarasını arttır ve paketi işlenmek üzere üst katmanlara ilet.

7 802.11 TELSİZ YEREL BİLGİSAYAR AĞLARI BENZETİM YAZILIMI

802.11i-2004 standardında getirilen yeniliklerin ve uygulanan güvenlik mekanizmalarının incelenmesi amacıyla bir benzetim yazılımı hazırlanmıştır. Benzetim yazılımı tek bir erişim noktası ve onunla haberleşecek istemcilerden oluşmakta ve kullanıcının istemcileri ve erişim noktasını yapılandırması, durumlarını incelemesi ve tanımlanan bir takım işlemleri gerçekleştirmesini sağlamak için bir arayüz kullanılmaktadır. Bu bölümde benzetim yazılımının özellikleri, kullanılan geliştirme ortamı, gerçekleştirdiği işlemler tanıtılacaktır.

7.1 Benzetim Yazılımı Geliştirme Ortamı

Benzetim yazılımı Linux işletim sitemi üzerinde geliştirilmiş ve Linux işletim sisteminde çalışacak şekilde tasarlanmıştır. Benzetim yazılımında istemcilerin ve erişim noktasının gerçeklenmesi için Kdevelop [28] entegre geliştirme ortamı (IDE-Integrated Development Environment) ve C programlama dili kullanılmıştır. Kdevelop geliştirme ortamı, derleyici (compiler) ve bağlayıcı (linker) olarak GNU/Linux derleyicisi olan gcc' yi (GNU Compiler Collection) kullanır. Hata ayıklayıcı (debugger) olarak Kdevelop entegre gdb (GNU Project Debugger) programı kullanılmıştır. Kullanıcı arayüzü, görsel kullanıcı arayüzü (GUI-Graphical User Interface) olacak şekilde Qt-Designer [29] programında tasarlanmış ve C++ programlama dili kullanılarak yine Kdevelop IDE kullanılarak gerçeklenmiştir [30].

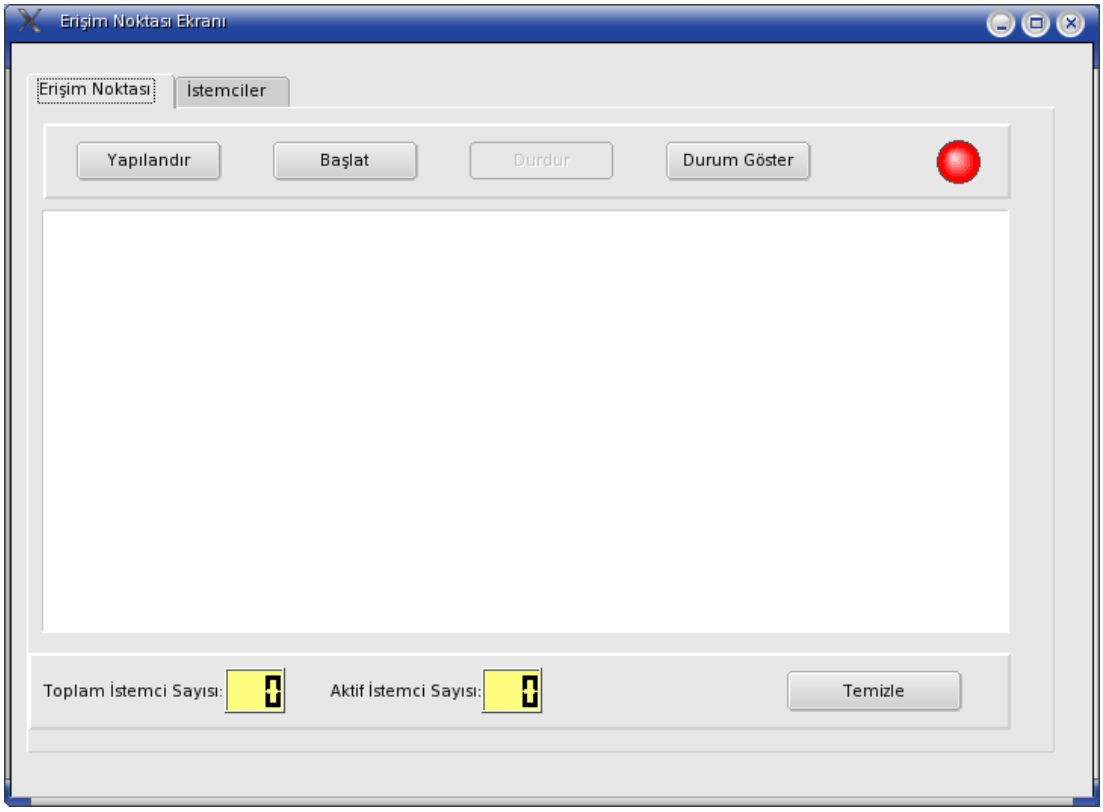
7.2 Benzetim Programı Modülleri

Hazırlanan benzetim programı toplam 3 modülden oluşmaktadır:

- Kullanıcı arayüzü
- Erişim noktası benzetimi
- İstemci benzetimi

7.2.1 Kullanıcı Arayüzü Modülü

Erişim noktası ve istemcilerin yapılandırılması, başlatılması, sonlandırılması, durumlarının sorgulanmasını sağlayan kullanıcı arayüzünün gerçeklendiği modüldür. Bu modül bir ana görev (process) ve bir görevcikten (thread) oluşur. Kullanıcı arayüzü ana ekranı Şekil 7-1' de verilmiştir.



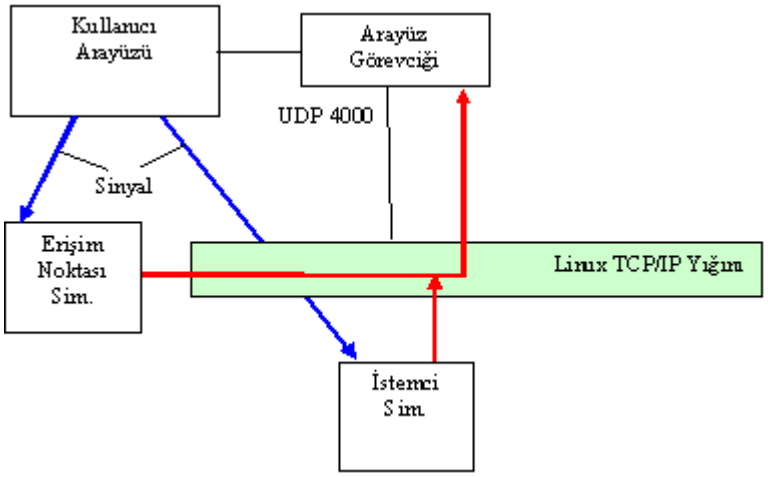
Şekil 7-1: Benzetim yazılımı ana ekranı

Kullanıcı arayüzü ile erişim noktası ve istemciler arasındaki haberleşme Linux işletim sitemi sistem çağrıları (örneğin yaratmak için "fork" ve "exec" gibi) ve erişim noktası ve istemci benzetimlerine gönderilen sinyaller (örneğin istemcilerin erişim noktasına veri göndermesini sağlayan "SIGUSR2" sinyali gibi) kullanılmıştır [31]. Tanımlı olan ve kullanılan sistem çağrıları ve yaptıkları işlemler aşağıda verilmiştir:

- Fork sistem çağrısı: Erişim noktası benzetimi veya yeni bir istemci benzetimi başlatılmak istendiğinde yürütülür.
- Exec sistem çağrısı: Yaratılan yeni görevin, yaratılma amacına göre (Erişim noktası veya yeni istemci) uygun benzetim programına aktarılmasını sağlar.

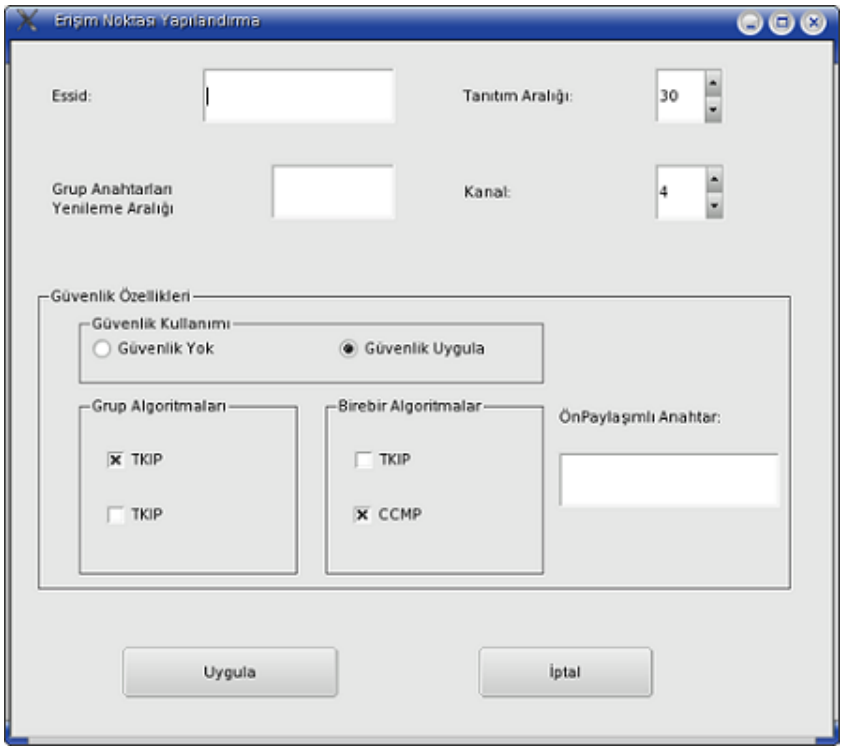
- SIGTERM sinyali: Erişim noktasının veya seçili istemcinin sonlandırılmak istendiğini bildirir. Bu sinyali alan erişim noktası kendinde bağlı tüm istemciler ile ilgili bilgileri siler, bu istemcilere kapandığını bildiren 802.11 yönetim mesajı gönderir ve sonlanır. Bu sinyali alan istemci kullandığı dinamik bellek alanlarını sisteme iade eder ve erişim noktasına kapandığını bildiren 802.11 yönetim mesajını gönderdikten sonra sonlanır.
- SIGUSR1 sinyali: Erişim noktası veya seçili istemcinin durumunu sorgulayan sinyaldir. Bu sinyali alan erişim noktası veya istemci o anda bulunduğu durum hakkında bir rapor oluşturur ve kullanıcı arayüzüne iletir.
- SIGUSR2 sinyali: Sadece istemcilere gönderilen bir sinyaldir. Bu sinyali alan istemci eğer erişim noktası ile haberleşme birliğini kurduysa haberleşme birliği uyarınca kullanacağı şifreleme ve özet algoritmalarını kullanarak erişim noktasına ICMP (Internet Control Message Protocol – Internet Kontrol Mesaj Protokolü) yankı isteğinde bulunur.

Kullanıcı arayüzü görevciği kullanıcı arayüzü yaratılırken oluşturulur ve kapatılırken sonlandırılır. Bu görevcik, istemciler veya erişim noktasına gönderilen sinyaller ve sistem çağrıları sonucunda bu benzetim programlarının oluşturacağı cevapları toplayarak kullanıcıya iletir. İstemcilerin ve erişim noktasının arayüz görevciğine veri göndermesi Linux TCP/IP yığını kullanılarak gerçekleştirilir. Görevcik başlatıldığında UDP 4000 numaralı portu açarak bu porta veri gelmesini bekler. Kullanıcı arayüzünden sinyal alan istemci veya erişim noktası benzetimleri istenilen işlemi gerçekleştirdikten sonra oluşturdukları raporu görevciğin dinlediği UDP 4000 numaralı porta gönderir. Arayüz görevciği bir anlamda syslog sunucu olarak UDP 4000 numaralı porta gelen karakter dizilerini kullanıcıya iletir. Kullanıcı arayüzü ve benzetim programlarının etkileşimi Şekil 7-2’ de gösterilmiştir:



Şekil 7-2: Kullanıcı arayüzü - benzetim öğeleri etkileşimi

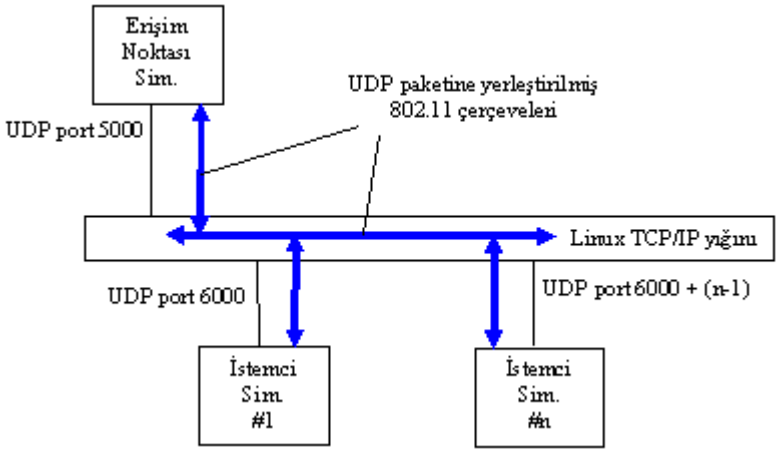
Kullanıcı arayüzü kullanılarak erişim noktası ve istemci benzetim programlarında kullanılacak yapılandırma dosyaları da hazırlanır. Kullanıcı arayüzünden girilen bilgiler belirli bir formatta yapılandırma dosyası olarak sabit diske kaydedilir. Erişim noktası ve istemci benzetim programları başlatıldığında öncelikle sabit diske kaydedilmiş bu yapılandırma dosyalarını açarak nasıl bir konfigürasyonla çalıştırmaları gerektiğini öğrenirler. Erişim noktası yapılandırma ekranı aşağıda verilmiştir. Benzer bir ekran da istemci yapılandırması için mevcuttur ve Şekil 7-3' de verilmiştir:



Şekil 7-3: Erişim noktası yapılandırma ekranı

7.2.2 Erişim Noktası Benzetim Modülü

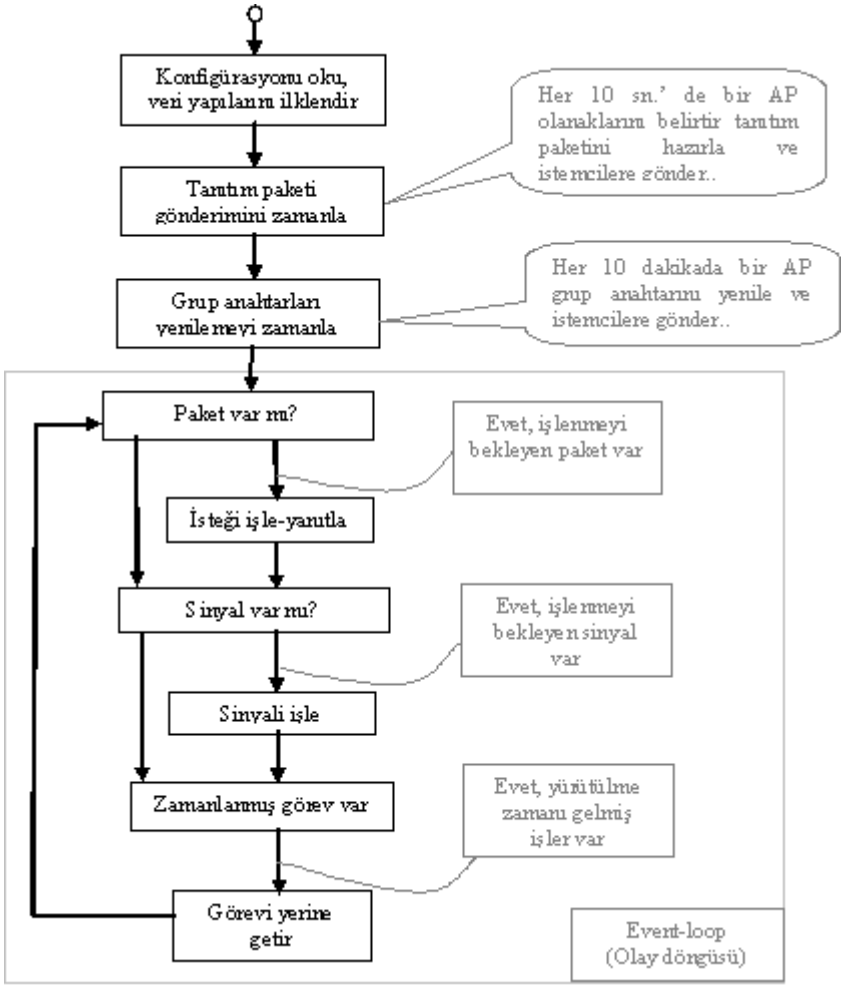
Erişim noktası benzetim programı 802.11 ağlarında erişim noktasının yapması gereken görevlerin benzetiminde kullanılan yazılımdır. Başlatılması, sonlandırılması ve yönetimi kullanıcı arayüzü üzerinden yapılır. Kullanıcı arayüzünden sinyaller alır, aldığı sinyallere uygun işlemleri gerçekleştirdikten sonra oluşturacağı raporu kullanıcı arayüzü görevciğinin işlemesi için UDP 4000 numaralı porta gönderir. İstemciler ile olan haberleşmesini de Linux TCP/IP yığını üzerinden gerçekleştirir. Erişim noktası başlatıldığında UDP 5000 numaralı portu açar ve bu porta gelecek istemci paketlerini dinlemeye başlar. İstemcilere göndereceği bir veri olduğunda UDP 6000-6099 aralığında tanımlı tüm istemci portlarına bu veriyi gönderir. İlgili istemci veriyi alır ve işler diğer istemciler kendilerine adreslenmemiş paketleri işlemeden atarlar. UDP 5000, 6000-6099 portları arasında gönderilen tüm veriler 802.11 standartlarına uygun olarak çerçevelenmiş yönetim ve veri mesajlarıdır. Erişim noktası benzetim programı ile istemci benzetim programları arasındaki mesaj alış-verişi Şekil 7-4' de verilmiştir:



Şekil 7-4: Erişim noktası benzetimi ile istemci benzetimleri arasında 802.11 çerçevelerinin aktarılması

Erişim noktası benzetimi kendisiyle haberleşen her bir istemci için ayrı bir veri yapısı tutar. Bu veri yapısında istemcinin anlık durumu varsa şifreleme ve özet anahtarları, yerel sıra numaraları gibi bilgiler bulunur. Erişim noktası benzetim programının temelinde Intersil firmasının ürettiği Prism II kırmık setli telsiz ağ adaptörünün Linux işletim sistemi için yazılmış sürücü programı (driver) yer alır [32].

Haberleşme birliklerinin kurulması, 4-yollu el sıkışma mekanizmasının gerçekleştirilmesi, veri gönderimi için TKIP veya CCMP kapsülleme işlemlerinin gerçekleştirilmesi, gibi oldukça karışık işlemler yapmasına karşın ana fonksiyonu çok basittir. Erişim noktası benzetim programı çalışmaya başladıktan sonra öncelikle yapılandırma dosyasını sabit diskten okur ve yapılan konfigürasyona göre veri yapılarını ilklendirir. Kullanıcı arayüzünden gelmesi muhtemel sinyalleri işleyebilmek için işletim sistemine ilgili sinyalleri yakalamak istediğini kaydeder, UDP 5000 numaralı portu açarak dinlemeye başlar ve sonlanıncaya kadar kalacağı "event-loop" (olay döngüsü) döngüsüne girer. Olay döngüsü içerisinde UDP 5000 numaralı porta paket geldiyse bu pakete ilişkin işlemleri yapar, sinyal aldıysa sinyale ilişkin işlemleri gerçekleştirir ve zamanlanmış görevler varsa bu görevleri yerine getirir. Erişim noktası benzetim programı ana fonksiyonu Şekil 7-5' de verilmiştir:



Şekil 7-5: Erişim Noktası benzetimi ana fonksiyon akış diyagramı

Zamanlanmış görevler gerçekleştirme sırasına göre en yakın görevden gerçekleştirilmesi en son yapılacak göreve doğru sıralı şekilde bir görev listesinde tutulur. Döngüde dönerken her seferinde zamanlanmış bir görevin gerçekleştirme zamanı gelip gelmediğine bakılır, geldiyse belirtilen fonksiyon belirtilen parametre ile çağrılır. Zamanlanmış görevler için tanımlı üç eleman vardır, gerçekleştirme zamanı, çağrılacak fonksiyon ve fonksiyona aktarılacak parametre. Zamanlanmış görevlere ilişkin tanımlı fonksiyonlar aşağıda verilmiştir:

- eloop-register-timeout(zaman, fonksiyon, parametre) : Hangi fonksiyonun ne kadar zaman sonra hangi parametre ile çağrılacağını belirtir. Çağrılacak fonksiyon çağrılma zamanına göre görev listesine eklenir.
- eloop-cancel-timeout(fonksiyon) : Belirtilen fonksiyona ilişkin tüm zamanlanmış çağrıların iptal edildiğini ve görev listesinden çıkarılacağını ifade eder.

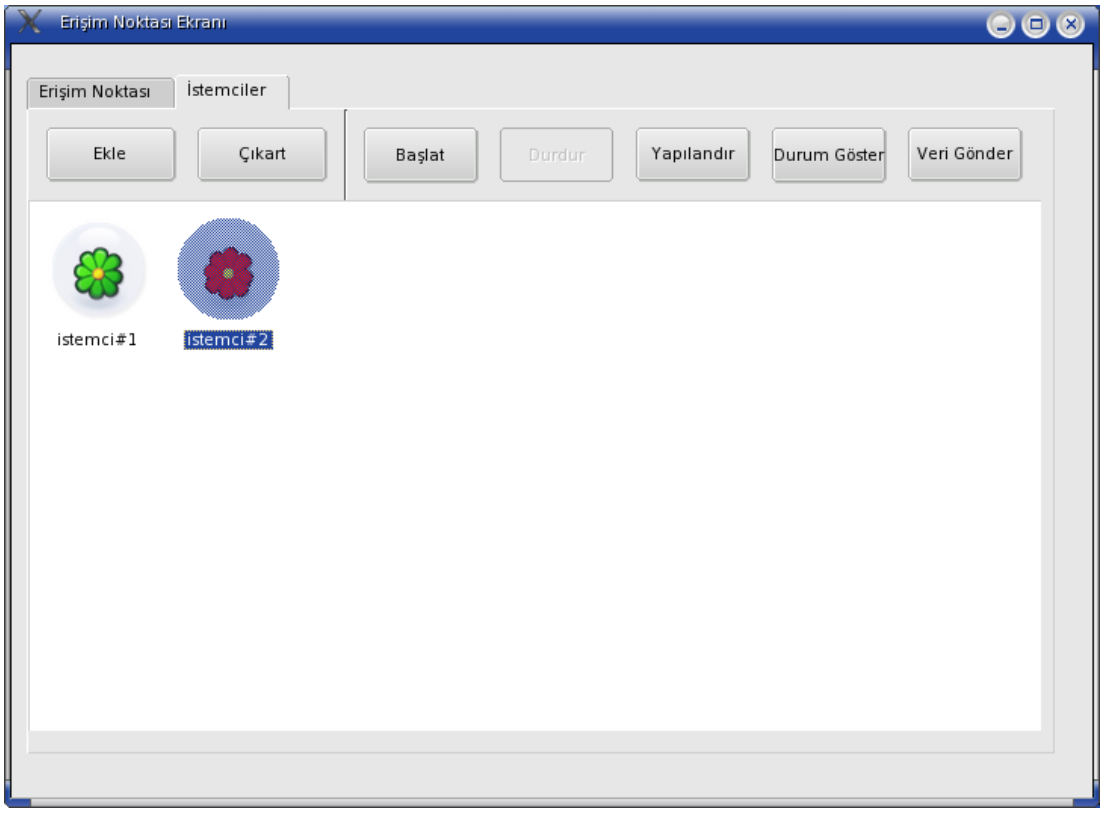
- eloop-timeout(fonksiyon, parametre) : Gerçekleştirme zamanı gelen fonksiyon belirtilen parametre ile çağrılır.

Erişim noktası benzetimi içerisinde iki farklı günlük tutma mekanizması mevcuttur. İlkinde Linux işletim siteminin "syslog" sistem çağrısını yürüterek günlük tutulur. Benzetim programı içerisinde farklı noktalarda farklı önem dereceleri taşıyan mesajlar mevcuttur. Kullanıcı istediği önem derecesini yapılandırma dosyası vasıtasıyla benzetim programına aktarır, toplam 5 faklı öncelik değeri mevcuttur. En düşük öncelik değeri ayarlandığında benzetim programındaki tüm mesajlar kaydedilir. En yüksek öncelikli mesajlar hata olması durumunda verilen mesajlardır. Benzetim programının günlük dosyası "syslog" sistem çağrısı ile tutulduğundan işletim sistemi tarafından "/var/log/users.log" dosyasına kaydedilir.

İkinci günlük tutma mekanizması UDP paketleri ile taşınan 802.11 çerçevelerinin kayıt altına alınması içindir. Erişim noktası tarafından gönderilen tüm 802.11 çerçeveleri paket analiz programı vasıtasıyla incelenmek amacıyla "libpcap" formatında formatlanarak günlük dosyasına yazılır. Paket analiz programı olarak "Ethereal" paket analiz programı kullanılmıştır. Böylelikle erişim noktasının gönderdiği tüm çerçevelerin standartlara uygunluğu analiz programı ile görüntülenebilir. Erişim noktası için paket günlük dosyası "/root/tmp/ap.dump" olacak şekilde seçilmiştir, ancak kaynak kod değiştirilerek istenilen dizine kaydedilmesi sağlanabilir.

7.2.3 İstemci Benzetim Modülü

İstemci benzetim programı, 802.11 telsiz ağlarında haberleşmede bulunan kullanıcıların benzetiminde kullanılan programdır. Erişim noktası ve kullanıcı arayüzleri ile ilgili arayüzleri önceki bölümlerde ele alınmıştır. Yönetilmeleri kullanıcı arayüzü üzerinden gerçekleştirilir, Şekil 7-6' da gösterilmiştir:



Şekil 7-6: İstemci benzetim programlarının yönetimi ekranı

Çalışma mantığı olarak erişim noktası ile benzer özellikler taşır, farklı olarak kullanıcıların yürütmesi gereken adımları yürütür.

Kullanıcı arayüzü, erişim noktası benzetimi ve istemci benzetimi programlarının kaynak kodları Ek-A' da CD (Compact Disc) olarak verilmiştir.

8 SONUÇLAR VE İLERİKİ ÇALIŞMALAR

Tez çalışmaları kapsamında hazırlanan benzetim programı ile IEEE 802.11i-2004 standardı güvenlik mekanizmaları ayrıntılı olarak gerçeklenmiş ve incelenmiştir. IEEE 802.11 telsiz yerel bilgisayar ağlarının IEEE 802.11-1999 standardı güvenlik mekanizmalarının zayıflığından kaynaklan sorunlarının giderildiği ve bilinen aktif ve pasif saldırılara karşı koyabilir duruma getirilmiş olduğu gözlenmiştir.

Benzetim yazılımı, hata ayıklayıcı (debugger) kullanılarak adım adım yürütülmüş olası zayıflıkların olabileceği noktaları bulabilmek için incelemeler yapılmıştır. Standarda uygun olmayan paketler oluşturularak 802.11i-2004 güvenlik mekanizmalarının verdiği cevaplar analiz edilmeye çalışılmıştır.

802.11i standardıyla getirilen 802.1X karşılıklı kimlik doğrulama adımı gerçeklenmese de paylaşılan anahtarla yürütülen 4 yollu el sıkışma mekanizmasının istemcinin erişim noktasını, erişim noktasının da istemciyi asıllaması için gerekli adımları başarı ve güvenle yürüttüğü gözlenmiştir. Karşılıklı asıllama ve anahtar yönetimi konusunda 802.11-1999 standardının oluşturduğu boşluk ve eksikliklerin kapatılarak güvenilir bir hale getirilmiş olduğu gözlenmiştir.

Karşılıklı asıllama da paylaşılan anahtarın kullanılabiliyor olması ev ve küçük ofis uygulamalarında kolaylıklar sağlayacaktır. Karşılıklı asıllama için kullanılacak olan 802.1X protokolü ile de ölçeklenebilir, genişletilebilir ve daha kolay yönetilebilir 802.11 telsiz yerel alan ağları kurulabilir.

Benzetim yazılımı ile gerçeklenen TKIP ve CCMP kapsülleme mekanizmalarının IEEE 802.11 telsiz ağları için gerek duyulan güvenlik önlemlerini başarıyla aldıkları ve aktif saldırıları engelleyebildikleri görülmüştür. Hali hazırda kurulu erişim noktaları ve istemcilerin yazılımları güncellenerek TKIP uyumlu hale getirilmesi önemle tavsiye edilir.

IEEE 802.11i-2004 standardı güvenlik mekanizmalarının kullanıcı veri paketleri için tanımlandığı ve yönetimsel mesajların herhangi bir şekilde korunmadığı fark edilmiştir. Yönetimsel mesajların taklit edilmesi suretiyle hizmet aksatmaya yönelik

aktif saldırılar gerçekleştirilebilir (DoS-Denail of Service). Yönetim mesajlarının güvenliğinin sağlanmamış olmasının yaratacağı problemler incelenebilir ve gerekli değişiklik önerilerinde bulunulabilir.

Benzetim yazılımının konu ile ilgili olarak yapılabilecek ileriki araştırmalar için bir alt yapı oluşturabileceğine inanılmaktadır. Gerek hata ayıklayıcılar kullanılarak benzetim programları adım adım yürütülebilir gerekse benzetim programlarının ikili dosya halleri ve kullanıcı arayüzü kullanılarak 802.11i-2004 standardı adımları incelenebilir. Benzetim programları arası haberleşme TCP/IP soketleri üzerinden gerçekleştirildiğinden istenmesi durumunda gerekli değişiklikler yapılarak benzetim programları farklı bilgisayarlarda çalıştırılarak başarım analizleri gerçekleştirilebilir.

Kullanıcı arayüzü ile erişim noktası ve istemci benzetimleri arası Linux işletim sistemi sinyalleri ile gerçekleştirilen senkronizasyon ve yönetim yerine geliştirilecek haberleşme protokolü ile benzetim programı istenirse başka işletim sistemleri altında da koşabilir hale getirilebilir.

Benzetim ortamında tek bir erişim noktası olacağı varsayılmış ve erişim noktaları arası geçişler (roaming) incelenmemiştir. Ancak istendiği takdirde gerekli değişiklikler yapılarak birde fazla erişim noktası benzetim programı çalıştırılabilir, IEEE 802.11f standardı olan erişim noktaları arası haberleşme protokolü eklenerek erişim noktası değiştirmeleri sırasında oluşabilecek güvenlik açıkları incelenebilir.

Telsiz yerel alan ağlarının başarılı bir şekilde büyümesi ve kullanıcıların ilgisini giderek artan oranda çekmesiyle ileride telsiz kampus ağları (WMAN) alanında da gelişmeler beklenmektedir. Belirli bir bölgeye kurulacak yüksek kazançlı antenler vasıtasıyla kullanıcılara Internet erişimi gibi hizmetler sağlanabilir. IEEE 802.16 bu konuda IEEE tarafından yürütülen çalışmaları kapsamaktadır. WMAN' ların kullanıma girmesi ile kablo çekmenin zor olduğu dağlık kesimler ve dağınık yerleşim noktalarına kolaylıkla erişilebilir. WMAN kullanımı da tıpkı telsiz yerel bilgisayar ağlarının kullanımı sırasında karşılaşılan güvenlik problemlerini de beraberinde getireceğinden şimdiden üzerinde durulması gereken bir konudur. Geniş kapsama alanı ve fazla sayıda kullanıcı için ihtiyaç duyulacak güvenlik mekanizmaları 802.11' den farklılıklar gösterebilir.

KAYNAKLAR

[1] **ANSI/IEEE Std 802.11**, 1999, Information technology-Telecommunication and Information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *IEEE Computer Society LAN MAN Standarts Commitee*, New York A.B.D.

[2] **IEEE Std 802.11i-2004**, 2004, Information technology-Telecommunication and Information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, *IEEE Computer Society LAN MAN Standarts Commitee*, New York A.B.D.

[3] **IEEE P802.11i/D3.0,** 2002, Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements- Specification for Enchanced Security, *IEEE Computer Society LAN MAN Standarts Commitee*, New York A.B.D.

[4] **IEEE P802.11i/D9.0,** 2004, IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks- Specific requirements Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enchancements, *IEEE Computer Society LAN MAN Standarts Commitee*, New York A.B.D.

[5] **Öztürk, E.,** 2004. WLAN Kablosuz Yerel Alan Ağları Teknolojisinin İncelenmesi, Mevcut Düzenlemelerin Değerlendirilmesi ve Ülkemize

Yönelik Düzenleme Önerisi, Telekomünikasyon Kurumu Uzmanlık Tezi, Ankara

[6] **Brenner, P.,** 1997. A Technical Tutorial on the IEEE 802.11 Protocol, http://www.sss-mag.com/pdf/802_11tut.pdf

[7] **Arbaugh ve diğ.,** 2001. Your 802.11 Wireless Network has No Clothes, *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*, Singapur, Aralık 2001, s. 131-144

[8] **Walker, J.,** 2000, Unsafe at any key size; An Analysis of the WEP encapsulation, *IEEE Document 802.11-00/362*, Oregon, A.B.D.

[9] **Borisov ve diğ.,** 2001, Intercepting Mobile Communications: The Insecurity of 802.11, *Proceedings of the seventh Annual International Conference on Mobile Computing and Networking*, Roma, Temmuz 2001, s. 180-189

[10] **Karygiannis, T. ve Owens, L.,** 2002, Wireless Network Security 802.11, Bluetooth and Handheld Devices, *Special Publication 800-48*, NIST Technology Administration U.S.Deparment of Commerce, Gaithersburg A.B.D.

[11] **Arbaugh, W.,** 2001, An inductive choosen plaintext attack against WEP/WEP2, *IEEE Document 802.11-01/230*, University of Maryland, College Park, A.B.D.

[12] **Edney, J. ve Arbaugh W.,** 2004, Real 802.11 Security Wi-Fi Protected Access and 802.11i, Addison-Wesley, Boston, A.B.D.

[13] **Fluhrer ve diğ.,** 2001, Weakness in The Key Scheduling Algorithm of RC4, *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto Kanada, 16-17 Ağustos 2001

[14] **Stublefield ve diğ.,** 2001, Using the Fluhrer, Martin, and Shamir Attack to Break WEP, *AT&T Labs Technical Report*, **TD-4ZCPZZ**, AT&T Labs., New Jersey, A.B.D.

[15] **IEEE Std 802.1X-2001,** 2001, IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control, *IEEE Computer Society LAN MAN Standarts Commitee*, New York A.B.D.

[16] **Blunk, L. ve Vollbrecht, J.,** PPP Extensible Authentication Protocol (EAP), RFC 2284

[17] **Aboba ve diğ.,** Extensible Authentication Protocol (EAP), RFC 3748

[18] **Dierks, T. ve Allen, C.,** The TLS Protocol Version 1.0, RFC 2246

[19] **Krawczyk ve diğ.,** HMAC: Keyed-Hashing for Message Auyhentication, RFC 2104

[20] **Rivest, R.,** The MD5 Message-Digest Algorithm, RFC 1321

[21] **FIPS 180-1,** 1995, Secure Hash Standart, *NIST*, Gaithersburg, A.B.D.

[22] **Schaad, J. ve Housley, R.,** Advanced Encryption Standart (AES) Key Wrap Algorithm, RFC 3394

[23] **FIPS 197,** 2001, Advanced Encryption Standart (AES), *NIST*, Gaithersburg, A.B.D.

[24] **Computer Security Resource Center,** http://csrc.nist.gov/CryptoToolkit/modes, 2005

[25] **Whiting ve diğ.,** Counter with CBC-MAC (CCM), RFC 3610

[26] **Kent, S. ve Atkinson, R.,** Security Architecture for the Internet Protocol, RFC 2401

[27] **Jonsson, J.**, 2002, On the Security of CTR + CBC-MAC, *Ninth Annual Workshop on Selected Areas in Cryptography*, Newfoundland Kanada, 15-16 Ağustos 2002

[28] **Kdevelop,** http://www.kdevelop.org, 2005

[29] **Qt Online documentation**, http://doc.trolltech.com/3.3 / , 2004

[30] **Qt Designer and Kdevelop,** http://women.kde.org/articles/tutorials/kdevelop3, 2004

[31] **Linux man Pages,** http://www.tldp.org/docs.html, 2005

[32] **Intersil Prism2/2.5/3 Linux Driver,** http://hostap.epitest.fi/, 2005

[33] **Bilişim Sözlüğü,** http://www.tbd.org.tr/index.php?module=dict, 2004

ÖZGEÇMİŞ

Zafer Bayraktar 14 Eylül 1978' de İstanbul' da doğdu. Ortaokul ve lise eğitimini İstanbul Bahçelievler Anadolu Lisesinde tamamladı ve 1996 yılında İstanbul Teknik Üniversitesi Kontrol ve Bilgisayar Mühendisliği bölümüne girdi. Lisans eğitimini 2001 yılında tamamladı ve aynı yıl İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği programında Yüksek Lisans eğitimine başladı. 2001 yılından bu yana TÜBİTAK-UEKAE' de araştırmacı olarak çalışmaktadır.